

ZVCHAIN

A High-performance, Highly Scalable, Next-generation
Enterprise Blockchain for Financial Services

Whitepaper v0.4.6



ZV CHAIN Founding Team

25 July 2019

Zi Wei Yuan

(The Purple Forbidden Enclosure)

Zi Wei Yuan, also known as Zi Wei Palace, is among the Three Enclosures in traditional Chinese astronomy. According to an early Chinese star catalogue, “Song of the Sky Pacers” (Bu Tian Ge), the Purple Forbidden Enclosure lies in the middle of the northern sky and is circled by the other two enclosures, thus it is also known as the “Middle Palace”. The Purple Forbidden Enclosure is centered at Polaris, with a total of fifteen stars, divided into the Left and the Right Wall in the constellation. In “History of Song: Book of Astronomy”, it remarks that “the Purple Forbidden Enclosure is to the North of Polaris, encircled by two lines of guarding stars, and it is a majestic sight to behold. ”

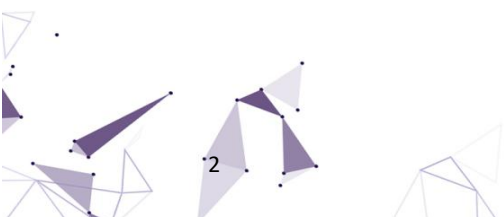
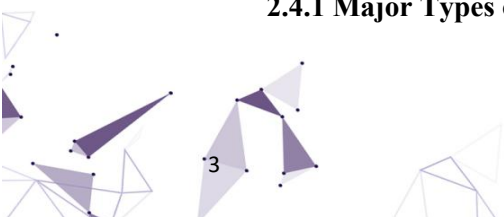




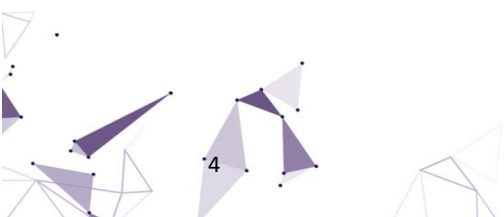
Table of Contents

CHAPTER ONE	5
Technical and Application Strategies of ZV CHAIN	5
1.1 High Security Layer 1	6
1.2 High Performance Layer 2	7
1.3 Specialized Middleware Layer	9
1.4 Application Layer	9
1.5 Smart Contract Support Modular Layer	10
CHAPTER TWO	12
The Innovative Design of ZV CHAIN	12
2.1 Chiron Consensus Mechanism	12
2.1.1 Open Participation Mechanism	15
2.1.2 Miner Incentive Mechanism	16
2.1.3 Group Chain Model and Block Chain Model	17
2.1.3.1 Group Chain Model	17
2.1.3.2 Block Chain model	22
2.1.4 Convergence Optimization and Communication Optimization	25
2.1.5 Forking	26
2.1.6 Checkpoint Mechanism	27
2.1.7 Consensus Analysis and System Security	28
2.1.7.1 Consensus analysis	29
2.1.7.2 System Security Analysis- Defence Against Attacks	29
2.2 Privacy-Preserving Computing and Security Framework	37
2.2.1 Data Privacy and Regulation	37
2.2.2 Formal Proof	41
2.3 Smart Contracts	42
2.3.1 Contract Upgrade	43
2.3.2 Major Anomaly Repair (Hard fork)	44
2.3.3 Efficient VM and Contract Language-Python	44
2.3.4 Financial Service Standardised Component Library and Component Market	44
2.4 Cross-chain Technology	45
2.4.1 Major Types of Cross-chain Technology	46





2.4.2 ZV CHAIN Cross-chain Protocol	48
CHAPTER THREE	50
ZV CHAIN Performance Optimisation Proposal	50
3.1 Sharding and Parallel Computing Framework	50
3.2 ZLight Lightning Network	52
3.2.1 ZLight Unidirectional Lightning Network	52
3.2.2 ZLight Bidirectional Lightning Network	52
3.2.3 ZLight Branch Structure	53
3.3 Distributed Data Storage	54
3.4 P2P Network	55
3.4.1 NAT Penetration	57
3.4.2 Multicast Network	58
3.4.3 RUDP	59
CHAPTER FOUR	60
The Technical Architecture of ZV CHAIN	60
4.1 ZV CHAIN Core Technology Architecture	60
4.2 ZV CHAIN Node Architecture	60
4.2.1 Node Categorisation	60
4.2.2 Node Function	63
4.2.3 Node Relations	64
CHAPTER FIVE	66
Technical Roadmap and Milestones	66
ZV CHAIN References	67
Appendix A: Technical Glossary	69
A.1 Chiron Consensus Terms and Symbols	69
A.2 Entities in the Settlement Network	71



CHAPTER ONE

Technical and Application Strategies of ZV CHAIN

ZV CHAIN has proposed a new type of consensus mechanism, Chiron, which employs Verifiable Random Function (VRF) true random numbers [1] to solve the problem of decentralization. At the same time, it rapidly achieves consensus through an interclass parallel operation, with a target Transactions-Per-Second (TPS) of 3000. Based on our years of extensive experience in the distributed system, we can assure a no single point design in the proposal, validation and block generation to further improve the performance and robustness of the system. Through rigorous mathematical computations and technical analysis, we believe that Chiron consensus mechanism provides the best solution to the Mundellian Trilemma till date, as shown in Figure 1.1.

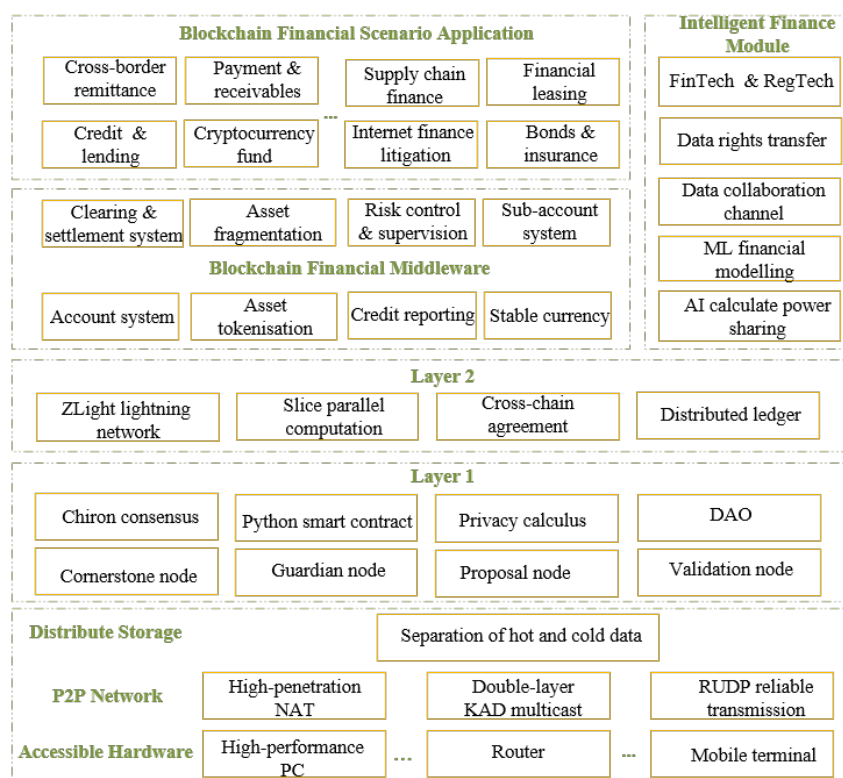


Figure 1.1 ZV CHAIN Technology and Application Strategies

We endeavor to build a convenient, highly secured and user-friendly decentralized network that everyone can easily participate in. Sustainable commercial applications can also be developed on this network at a minimal cost. By introducing mathematics, cryptology and engineering technology into the

network, it ensures its decentralization and high security, as well as achieve a high performance at low energy cost.

1.1 High Security Layer 1

In Layer 1, our developed consensus mechanism Chiron uses a Verifiable Random Function+Boneh-Lynn-Shacham (VRF+BLS) working mechanism. The grouped VRF ensures that private mining is not possible and shields itself from long-range attacks. It also increases the requirement for a 51% attack to a 95% control of the total nodes. Furthermore, the POS interest stake is linearly related to block generation rewards, securing the network against sybil attacks by overcoming disinterested relationships through a reward and penalty system. The application layer is also designed for group communications. For scenarios that require safety communication channels, safety is guaranteed through the Elliptic-curve Diffie–Hellman (ECDH) algorithm that encrypts communication channels. To ensure security in the user accounts, we use a zero-knowledge proof technology to safeguard account security and privacy protection. After a smart contract is submitted, the system will conduct an in-form validation of the smart contract to audit the safety of the contract. This will ensure its safety during the execution process. ZV CHAIN categorizes the various equipment into two types: light nodes and heavy nodes. Based on the amount of contribution by miners to the ZV CHAIN network, a miner health index will be generated. ZV Chain adopts a grouped consensus protocol with integrated true random number computation (VRF and BLS).

ZV CHAIN uses consensus mechanism with integrated technology. It combines VRF+BLS and introduces several technologies in the distributed system, such as sharding, high concurrency collaboration and preprocessing. Its basic principle of design is as follows: The system can increase its throughput by increasing the number of nodes. Currently, sharding is deemed the most optimal solution. The consensus mechanism must therefore support the sharding process and is best facilitated through a grouping of the miners.

This method of grouping the miners, however, presents a great risk of collaborated perpetration by group members. Thus, a VRF secret ballot will be used to randomly select the proposal group and send the candidate blocks to the validation group. The candidate block in the validation group that first achieves the threshold signature will be the winner. This mechanism of a concurrency collaboration significantly reduces the chances of a collaborated perpetration. The efficiency of the validation also reflects the processing performance of the system. Taking into consideration the complication of communication, the



length of signature and performance, we believe the validation group using the Boneh–Lynn–Shacham (BLS) threshold signature will perform better than another using the Group Byzantine Fault Tolerance. Even for scenarios similar to the optimization of Zilliqa on Practical Byzantine Fault Tolerance (PBFT), the results achieved are close to the threshold signature but never surpassing it.

- Customized Virtual Machine (VM)

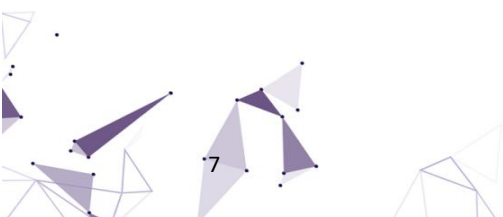
Currently, most blockchain systems that support smart contracts uses VM with stack architecture. Stack architecture resolves the problem of consistency among the various physical operating systems, but also leads to a lowered efficiency in operations. The TVM of ZV CHAIN is based on LLVM. On the basis of ensuring consistency and scalability, it significantly improves the running efficiency of the contract.


- Privacy-preserving Computing

Privacy-preserving computing [2] achieves the secured processing of data under the premise of protecting data privacy through technical means. From the perspective of cryptology, privacy-preserving computing is the use of modern computing methodology as represented by a secured multi-party computation and a homomorphic encryption. Analysis and computing of data is achieved while protecting the security and privacy of the original data. To guarantee account security and privacy protection, the zero-knowledge proof (ZKP) technology is used; a prover can make a verifier believe a certain conclusion is right without providing any usable information to the verifier. Thus, the prover proves to the verifier and the verifier believes that the prover knows or owns certain information. During the proving process, no information on the piece of news to be proven is revealed to the verifier. The privacy of public blockchain will be further improved through the use of ZKPs technology. Other than the validity of the disclaimer, no other information will be revealed during the proving process. The application can be applied to blockchain to camouflage the identity of traders and the trading volumes. It also ensures user account security and privacy protection. For data storage security and privacy protection, we employ the homomorphic encryption.

1.2 High Performance Layer 2

During the early stages of design in ZV CHAIN, we have already considered the cost of system efficiency in order to appropriately tap on the hash power of the full-network. In the sharding mechanism





[3], the Chiron consensus mechanism uses the strategy of grouping and supports the sharding of Layer 2 from protocol level, performing the computing framework.[4] Layer 2 randomly selects certain groups for sharding and computing. The other idling groups will periodically execute a checkpoint and validate the veracity of the blockchain data. At the same time, ZV CHAIN draws on the principle of fractionated processing. It uses cold and hot backup for system data (account, trade, smart contract, etc). Most of the nodes only require storage for hot data. This improves the cost efficiency for data storage.

- Sharding and computing

ZV CHAIN borrows its knowledge from Google MapReduce and Batch computing from AliCloud to design an executional framework for sharding and trading. It also supports data sharding processing. The VFR grouping mechanism ensures that different groups can execute different tasks in parallel, thus increasing the system throughput by one order of magnitude.

- ZLight Lightning Network

As a professional finance public chain, incorporating Lightning Network not only improves the system's throughput, but also forms an integral part of the branching architecture. Thus, the ZLight Lightning Network was developed. The ZLight Lightning Network can securely execute trades in the funding account offline with its only requirement being periodical settlement and synchronization with the main chain. Frequent small trades do not need to be put on the chain in real time. The lightning network can quickly build convenient and light connections between business and consumers through the ZV CHAIN and complete the deals in high security.

- Storage of distributed ledger

All existing blockchain projects, be it Ethereum or Bitcoin, require full data storage for their mining nodes. The data will accumulate over time and the nodes take up hundreds of gigabytes or even terabytes of data on storage, marking a huge waste in storage. At the same time, performing a cold boot for the new nodes will take a very long time. We think that browsing historical data is a low-frequency operation. Learning and acquiring the guiding principles from Cassandra, HBase and other column-based distributed storage systems as well as certain projects by Alibaba that separate cold and hot data, we intend to optimize the storage of data in blockchain. In Phase 1, we plan to build a full ledger storage with heavy nodes. In Phase 2, we will realize the distributed storage of full ledger with heavy nodes. These heavy nodes will be responsible for the block generation proposal. Light nodes will only store part of the ledgers and the relevant statuses of recent block height accounts. It will validate and sign the candidate blocks under a group



coordination. Even if a mobile phone is used as a light node, it can still participate in ZV CHAIN block generation with the supporting packaged App.

1.3 Specialized Middleware Layer

For a better and easier adoption in the finance industry, we will extract some universal utility modules customized for potential application in finance industry. We will develop multiple middleware in different stages with the purpose of improving security and performance. DAPP's developers can also conveniently obtain relevant middleware support by invoking the API.

- Payment Settlement Solution

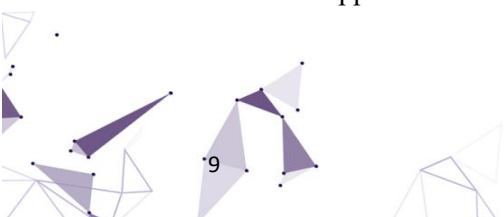
A payment settlement solution based on ZV Chain will make use of the distributed ledger and Lightning Network to enhance efficiency in exchange of information and clearance for users, businesses and corporates. It may define a unified technological and functional standard for security and reliability of financial network activities. In the scenario of cross-border clearance, it will be performed by proxy nodes and a two-way Lightning Network. The proxy nodes may support fiat-backed stable coins accepted by local merchants and the ZV CHAIN tokens as the final clearance tools.

- Risk Control Solution

Risk control is the lifeline of any finance application. The effectiveness of risk management often determines the success of a financial application. Most of the advanced risk control systems are based on huge amounts of historical and real-time data to build a smart rules engine and risk management model to exercise risk control. Risk management involves dealing with large amounts of private data from users and company trade secrets. Thus, these confidential data cannot be put on the chain directly. Through the risk control oracle interface, the on-chain smart contract is able to obtain a risk assessment and execute its respective operations based on risk control.

1.4 Application Layer

Considering the disparity in financial scenarios and user requirements [5], there are two possible modes of application solutions - Baas (Blockchain as a Service) [6] and DAPP's development - to meet





the needs of different users at different business operational scales. Various applications can be adapted according to the specific circumstances:

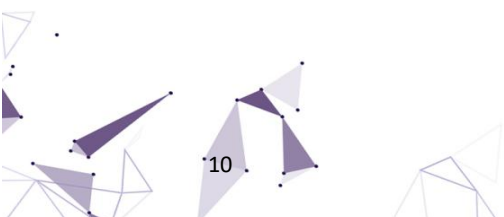
- Supply Chain Finance
- Financial Leasing
- Internet Finance Litigation
- Payment and Cross-border Remittance
- Tokenization of Off-chain Assets
- Credit & Lending
- Bond Issuance and Insurance
- Crypto Fund

1.5 Smart Contract Support Modular Layer

The three key elements for implementing Artificial Intelligence (AI) are robotic learning algorithm or model, big data and high-performance hash power. In recent years, most of the industries have transited to big data and begin their transformation to AI, especially in the financial sectors. The potential of smart financial services has been acknowledged by more and more authorities. However, traditional centralized IT architecture also contains many problems, such as the leaking of private data, the collecting of user data by centralized platforms for commercial applications, and the inability to effectively protect innovation, etc. To tackle these problems, many industries set their eyes on the rapidly evolving blockchain technology and its applications in an attempt to transit to a decentralized blockchain infrastructure. At the same time, as an internet protocol-level infrastructure that enables financial value connection, blockchain by itself is insufficient to meet the requirement of a smart financial service. Thus, we have incorporated big data processing modules, a machine learning algorithm library and the AI hash power. We will provide comprehensive architectural support to build smart financial modules on the public chain protocol layer.

In addition, we intend to provide support to the coordinated invoking of data, hash and models in the blockchain financial middleware.

- Data coordination channel





Data coordination channel provides big data exchange both inside and outside of the blockchain. On one hand, it can connect to external data of different types and dimensions to provide data support for training smart models. On the other hand, it creates the condition for the value flow of authenticated public chain data.

- AI Hash Sharing

Based on the architecture of the public chain protocol layer, the sharing functions of high-performance devices will be developed. This will improve the utilization of on-chain high performance devices and fulfill the needs of the public chain users to develop smart financial models.

- ML financial model library

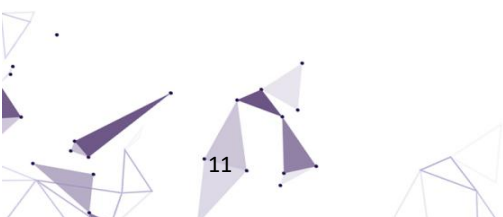
Through the sharing of swarm intelligence, in particular the smart model training “intelligence” from the on-chain robotic learning expert, we will provide a financial model library for a multitude of complex smart financial services. Public DAPP’s users with similar requirements can use these services at their convenience.

- Data authentication and value flow

Firstly, user data protection and authentication can be realized through many protocol layer public chain privacy computing modules. Subsequently, trading and usage channels will be provided for paid authorized data. Authorized users will receive a reward for their data sharing. Finally, based on the output of the shared data training, the process of the data value flow will be completed.

- FinTech and RegTech

We will develop different smart services through the robotic learning financial models as mentioned above. This will meet the various needs of traditional financial services and aid in the upgrading of traditional financial regulations, truly realizing the vision of Fintech and RegTech.





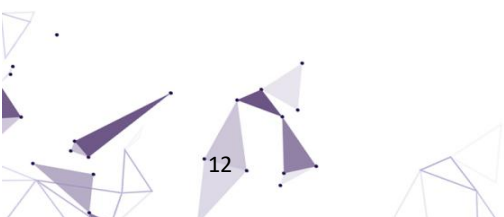
CHAPTER TWO

The Innovative Design of ZV CHAIN

2.1 Chiron Consensus Mechanism

Since the birth of Bitcoin, there has been continuous research on the blockchain consensus mechanism from both academia and the industry. Many different mechanisms, protocols and algorithms have been established. With all these developments, however, one challenge remains unsolved--the trilemma to fulfill decentralization, security and performance. POW (Proof of Work) suffers from low-performance mechanism and high energy consumption. POS (Proof of Stake) cannot take care of both decentralization and performance at the same time. HASH and DAG target more on consistency rather than accuracy. These consensus mechanisms will normally pick two verticals from decentralization, security and performance to enhance. As a result, they seldom consider the optimal solution for the bigger picture. Some consensus mechanisms are leaning more towards the academic aspect. Consequently, many mature technologies that prosper in the internet, such as decentralized collaboration, layered processing, preprocessing and multi-level cache, are not effectively integrated into blockchain. In addition, few consensus mechanisms have conducted thorough analysis and contention on security problems such as Nothing-at-Stake, 51% attacks, sybil attacks and long-range attacks. With ZV Chain, we have developed a brand-new consensus mechanism, Chiron. It combines VRF and BLS and introduced various technologies in decentralized system, including sharding, high concurrency collaboration, preprocessing and others. Chiron consensus mechanism takes random samples from the light node miners and put them into several validation groups generated by the collaborated VRF algorithm to determine the validation group in each round. Full node miners on the blockchain nominate proposal groups through secret balloting, and send the candidate blocks to the validation group, which then validate the candidate blocks and determine the final block through a group collaboration.

Chiron consensus mechanism has several key strengths. In terms of decentralization, it outperforms Bitcoin as it can mobilize any network device as a potential node. At the same time, Chiron incorporates light and heavy nodes to cover both the breadth and the depth. In terms of security, validation groups are selected through VRF-generated true random numbers, guaranteeing the uniqueness of the working group at a particular block height and eliminating the possibilities of long-range attacks and



unauthorized mining activities. One has to control at least 95% of the nodes to initiate an attack similar to the 51% hashing attack on Bitcoin. In terms of performance, Chiron targets TPS 3000 without sharding or optimization. Chiron incorporates a series of mathematical tools, cryptographic algorithms and comprehensive protocols. Its core mechanism can be summarized as follows: light nodes and miner nodes are grouped--usually 100 nodes per group. Whenever a block is mined, a proposal group is selected randomly by full nodes through VRF algorithm. This renders the proposer random and unpredictable, curtailing the risk of collusive fraud between the proposer and the verifier. The proposal will be sent to the verification committee through multiple channels concurrently. The verification group is selected by VRF, which is based on the threshold signature scheme. This ascertain the unpredictability, randomness and transparency of the verification committee. During the actual block generation, only light inter-group verification is required to achieve rapid block generation through concurrent multi-channel production lines.

By comparing with frontier public chains, the advantages of Chiron can be clearly seen in almost every major aspect.

Table 2.1 Comparison with Mainstream and Upcoming Public Chain

		Decentralization	Security	Performance
ZV CHAIN	BTC	✓	✓	✓
	EOS	✓	✓	
	Dfinity		✓	✓
	Algorand		✓	✓
	Cardano		✓	✓
	Zilliqa		✓	✓

Chiron surpasses BTC in terms of its enhanced decentralization and strengthened security as well as significantly upgraded performance and drastically lowered energy consumption. Comparing with EOS, Chiron stands at the same level in performance, but boasts a clear edge in terms of decentralization and

security. We contend that in the context of the blockchain system, decentralization takes higher priority over security which in turn precedes performance.[7] Compared with Dfinity [8], Chiron is equally competent in terms of decentralization, yet it deploys small distributed collaborative bodies within groups in order to enable highly efficiently inter-group task divisions and collaborations, enhancing its performance and robustness. The proposer is randomly selected by full node VRF secret balloting mechanism. The difficulty level of a collusive fraud between the proposer and the verifier is therefore increased from group level to full network level, thereby substantially curbing the possibility of collusive frauds. Compared with Algorand, the grouped VRF relay model has a unique and unpredictable validation group to map at every block height. Block candidates broadcast in a directed way to verification groups. Intra-group consensus is achieved through BLS threshold signature to perform validation. Therefore, Chiron is far ahead of Algorand in terms of communications, the size of the signature data and performance. Compared with Cardano, all nodes in the Chiron network can participate in block generation. Every step during block generation is mirrored to eliminate single points of failure. As illustrated in Figure 2.1, by improving the robustness of the system, the average performance is significantly boosted.

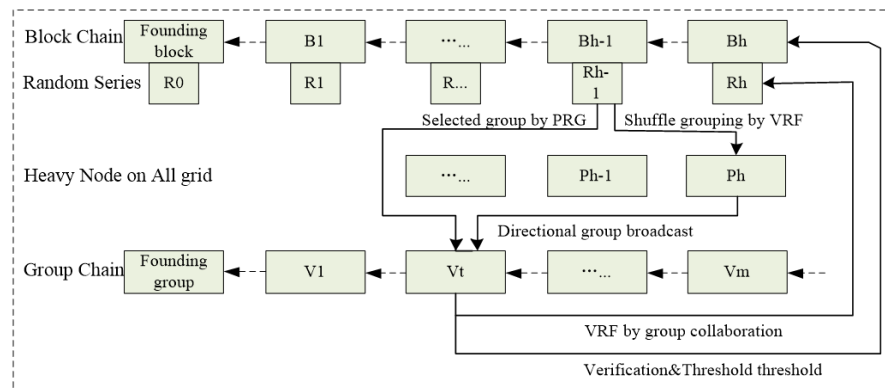


Figure 2.1 The Block Generation Process of Chiron

Compared with Zilliqa, all members in the verification group of Chiron will be able to recover the final group signature after receiving the threshold signature. The final multi-signature aggregation can be realized without having to appoint a leader within the group, thus enhancing the robustness and the security of the system. From the above comparison with major and emerging public chains and by showing mathematical and formal proofs, we can conclude that the Chiron consensus mechanism is the most optimal solution to the “impossible trinity” problem in the consensus algorithm. Chiron is leaps and strides ahead of all existing consensus mechanisms.



To ensure orderly operation of the system, we have made the following assumptions on the parameters of the miners:

1. Both honest and malicious miners exist in the system.
2. Honest miners outnumber malicious miners.
3. Both honest and malicious miners are driven by economic gains. Honest miners' profit by observing the rules, while malicious miners profit more by breaking the rules.

2.1.1 Open Participation Mechanism

The Chiron consensus mechanism employs open participation mechanism that allows average users to apply to access the system and become miners. On the other hand, miners can also apply for annulment and reclaim their user status. For these actions, we have designed specialized smart contracts, the Miner Application Contract and the Miner Annulment Contract. Both contracts are inscribed in the genesis block to be called by the users.

Miner Registration

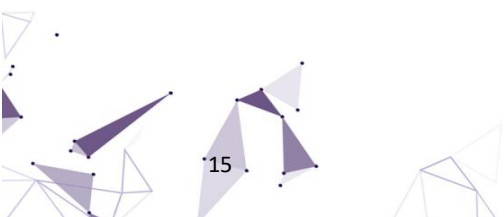
During the application process, a normal user needs to submit a Miner Application Contract, indicating the type of miner they intend to apply for, i.e. proposing miner or validating miner. Every miner has a unique ID.

$$\text{ID} = \text{transhash}(\text{pk})$$

“pk” is the public key of the user before he becomes a miner. *transhash* currently uses a hash function that outputs 256-bit. The public key of the user corresponds to his miner ID and is unique in the system. The Miner Application Contract codes (pk, Type) into the blockchain. In principle, miners on heavy nodes are expected to become proposing miners, while those on light nodes are expected to become validating miners.

Miner Annulment Contract

Miners can submit the Miner Annulment Contract to withdraw from the Chiron consensus. Similarly, the annulment contract will be inscribed into the blockchain. After a period of time (longer than the group's life cycle), as illustrated in Figure 2.2, users can call upon the deposit to redeem their contract. The deposit will be released to the users by the system. The Chiron consensus uses random sampling on light node miners to create several validating groups.



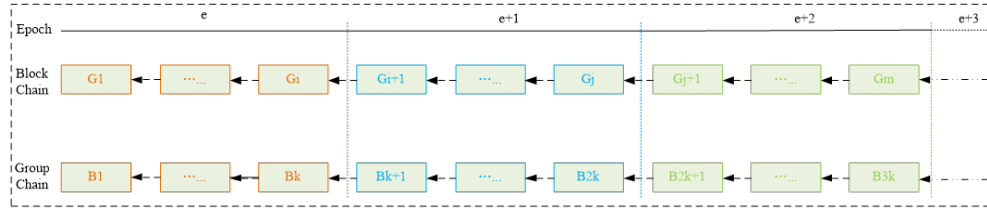


Fig 2.2: The Demarcation of Chiron Group Cycle

Real random numbers generated by the grouped VRF algorithm serve as random seeds for the PRG function, which in turn generates random numbers that determine the validating group for the current slot. Heavy nodes across the network are grouped in accordance with the random numbers of the previous block and the proposal group for the current slot is selected randomly. Members of the proposal group nominate several candidates block and broadcast it to the validating group, who will then complete the block validating process through group collaboration. The validating group will subsequently establish an intra-group consensus through the threshold signature before broadcasting it to the entire blockchain. Owing to the immutability and traceability of the data as shown in the figure above, the Chiron consensus utilizes a dual-chain model, namely blockchain and group chain, to document the production of the entire data chain. To curb the possibility of collusive frauds within the group, each group has a life cycle and will be dismantled for a new round of random sampling and grouping process. After the system stabilizes, whenever it enters a new epoch, new groups will be formed, and the old ones will be dismantled. Therefore, in every epoch, the working list will vary accordingly.

2.1.2 Miner Incentive Mechanism

To motivate and reward miners and ensure that the project is steered towards a positive direction, the design of ZV CHAIN must incorporate an economic incentive mechanism. The economic incentive model should have a remuneration system that reasonably compensates the miners for their hard work while remaining consistent, auditable, traceable, impartial and immutable. The description above mirrors a contract of service found in traditional businesses, and it is for that very reason that our smart contract is designed. Naturally, a smart contract is the best solution to concretizing theoretical economic incentive models.

The ZV CHAIN system initiates a specialized smart contract at the beginning of each new round of block generation. Miners who contribute to block generation, including proposal or validation, can call the contract with proof of work after they have tallied the work that is completed in this round. The

remuneration is calculated based on the smart contract, which functions as a proof of work. After a window period, the logic of reward in the contract will be triggered automatically and will transfer the reward to an individual miner's account, as illustrated in Figure 2.3.

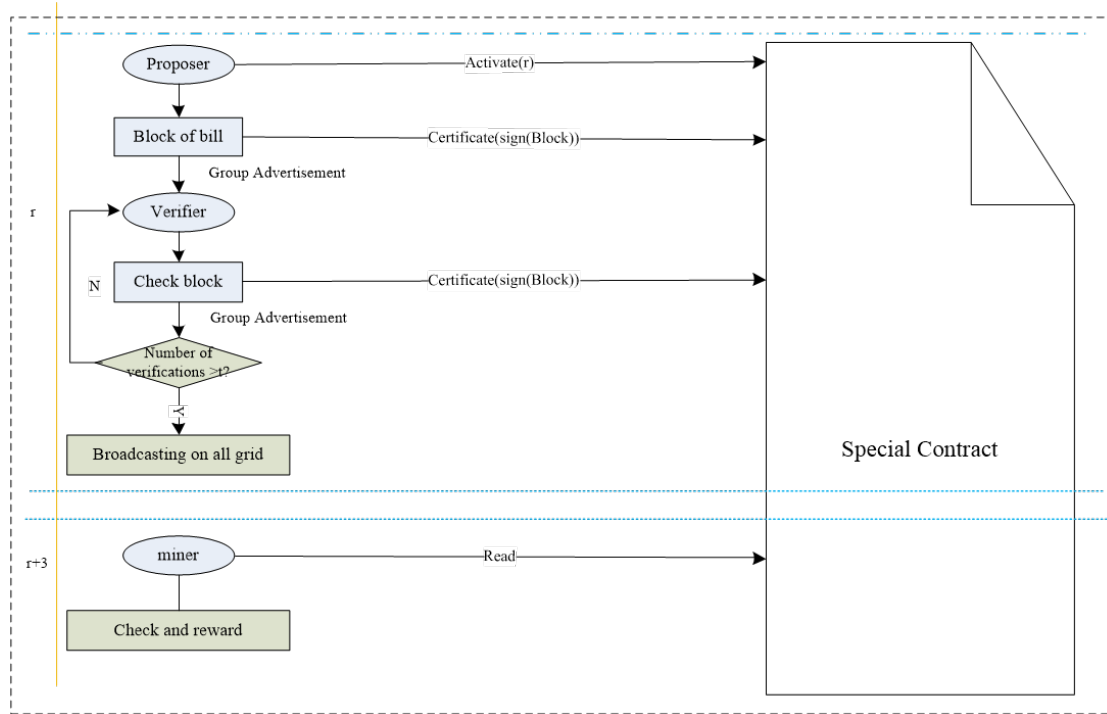


Figure 2.3 The Economic Reward Flowchart of Chiron

ZV CHAIN mobilizes smart contract to concretize the economic incentive model, not only in a secure and impartial manner, but also to provide fundamental statistics that lay the groundwork for creating and evaluating crucial indexes such as the health index of each mining node. Based on the statistics, we can easily distinguish positive miners from negative ones. The health index contributes positive feedback to further computations done by Chiron on future mining activities.

2.1.3 Group Chain Model and Block Chain Model

2.1.3.1 Group Chain Model

1. Data Structure of Group Block

- Type: Miner type (proposal or validation)
- Hash: Group block hash value
- GIS: Information specified by Parent group (refer to Section 2 for definition)

- Activation: the epoch when the group is activated
- Deactivation: the epoch when the group is deactivated
- MinerArray[]: the set of candidate blocks
 - *pubk*: miner's corresponding public key
 - ID: miner's identification
- Signature: parent group's signature on GIS
- Prehash: the hash value of parent group
- Gpk: group public key

2. Group Building and Maintenance

ZV CHAIN system carries out regular checks on group building based on CheckInterval (a system parameter). Suppose it is currently in the r^{th} round slot, if r is a multiple of CheckInterval, when a new block is generated, the current working group should undergo group building and maintenance. Considering the problem of chain synchronization, and assuming that it takes d slot timing to broadcast to the entire network, it is safe to conclude that blocks before the d^{th} block are already in sync. Thus, it can be concluded that all blocks across the network at a height no higher than $r-d$ are perfectly in sync. Through an examination of the miner contracts and a deliberate screening mechanism, members of the working group can determine the number of suitable candidates who meet the requirements to be a part of the new group. The working group will thus be a parent group to the new group formed and raise proposals for forming new groups accordingly.

3. New Group Proposal

Being the parent group, the current working group raises proposals with the main goal to determine potential candidates for the new group. The key strategy is to rank candidates according to their health index, before generating pseudo-random-number sequences with real random numbers of the current block as seeds. The random selection of candidates guarantees that the distribution of health index among the new members is similar to that of all suitable candidates and that some members with high health index will carry along some members with low health index. By doing so, it eliminates the probability of being attacked by “zombies”. In addition, the current working group must decide the activation time of the subsequent new group. For example, in the second epoch after the current epoch e , $GIS.Activation = e+2$, the deactivation of the new group is dependent on a system preset parameter, ValidPeriod. $GIS.deactivation = GIS.activation + ValidPeriod$. Owing to the aforementioned candidate sequence, new member selection



strategies are auditable. As a result, the hash calculated should be the same for all honest miners in the current group. Each miner within the group can thus generate and sign on their individual hash and corresponding information before sending it to the rest of the group. Once the hash received equals to or exceeds the threshold, group members can use the group signature to recover the output private key to sign on the group block. The parent group will also call the bonus smart contract template on the genesis block to establish a bonus contract and then publish it for the new group. The contract will eventually be written in the blockchain.

4. Establishing New Group

In reality, as group members are peer nodes on the decentralized network, sometimes it is inevitable that some nodes have to go offline due to unforeseeable circumstances, such as unstable network connection, malicious nodes, etc. To prepare for the unpredictable, the verification group is designed to have (t, n) threshold signature capability, where n refers to the number of group members, and t the threshold value (usually $t \leq n$). This means that group consensus is achieved if the number of group members who has signed their acknowledgement is greater than the threshold value, and the group signature can be recovered from the agreement among the t members. We employ a decentralized form of sharing - Shamir's Secret Sharing, to generate signature private key S among group members, group signature public key, and group public key gpk as opposed to group private key which represents group consensus. Once these private keys are obtained, and the consensus on public key is agreed upon, the group is hereby established.

The classical Shamir's Secret Sharing algorithm [9] can be perceived as a process seeking "centralization", as it requires a "dealer" who decides on the what secret polynomial to use. The dealer then fragments the secret and disseminate it to others. However, blockchain is a decentralized network. Every node is equal and no centralized "dealer" should be elected from peer nodes. In addition, the "dealer" precedes others in knowing the secret, therefore it is hard to prevent wrongdoings if the "dealer" has malignant intents. In view of these intrinsic flaws, we employ a decentralized private key sharing algorithm. Its core principle lies in empowering every group member to become the "nucleus", or the secret dealer. As a result, there is no physical "centralization". But at the same time, an initial secret is formed at the logic layer of the group. None of the members has knowledge of this secret. By following the three steps listed below, every member will be able to form a shared secret S_i in the group logic layer. Similar to the classical Shamir's Secret Sharing algorithm, the set of shared secret, S_i , is able to reconstruct the secret SK when the threshold is met, i.e. the initial secret SK can be reconstructed by obtaining no



less than t number of secret shares. In the case that the total number of secret shares obtained is less than t , no information about the initial secret SK will be distributed at all.

Specific implementation steps are as follow:

- a) Each member chooses his individual secret sharing polynomial

$$f_i(x) = a_{i,0}x + a_{i,1}x^2 + \dots + a_{i,t-1}x^{t-1}$$

Polynomial coefficients $a_{i,0}, a_{i,1}, a_{i,2} \dots a_{i,t-1} \in GF(p)$ are randomly chosen by individual group members. Hence every member's initial secret is $sk_i = f_i(0) = a_{i,0}$. Using the private key sk_i , the corresponding public key pk_i is calculated.

- b) Each member computes the shared secrets to be allocated to other members and sends them respectively, that is the i^{th} member computes $S_{i,j} = f_i(ID_j)$ and sends to the j^{th} member, together with his public key pk_i , where $i = 1, 2, \dots, n; j = 1, 2, \dots, n$;
- c) When a member collects all shares of secrets from other group members, he can compute the sum of all secret shares he has received $S_i = \sum_{j=1}^n S_{i,j} = \sum_{j=1}^n f_j(ID_i)$, and calculate $gpk = \sum_{j=1}^n pk_j$
- d) Each member calculates mpk_i , the public key corresponding to the private key of the group signature, and informs other members of the mpk_i

Note: in step (b), the communication among group members should be encrypted to prevent it from being wiretapped. The corresponding user public keys $pubk$ of all the miners within the group are recorded in the new hash information set, MinerArray, which will be used as the ECDH key for encrypted communication.

After completing the above steps, each member obtains a private key for the group signature, S_i , a public key, mpk_i , and the group public key gpk that corresponds to the group private key SK . The group logical layer also harbors the group private key $Sk = \sum_{i=1}^n sk_i$. As every member is only privy to his own initial secret, sk_i . SK , therefore, remains unknown.



We will prove that SK can be reconstructed from member private key S_i if the threshold is fulfilled.

(a) Proof of Correctness

As the sequence of group members is inconsequential, we assume that k refers to the first k members, for any $k \geq t$. Let $F(x) = \sum_{i=1}^n f_i(x)$, from Lagrange interpolation polynomial $G(x) = \sum_{i=1}^k S_i \prod_{j=1, j \neq i}^k \frac{x-ID_j}{ID_i-ID_j}$, which holds for $1 \leq i \leq k$.

$$F(ID_i) = \sum_{j=1}^n f_j(ID_i) = \sum_{j=1}^k S_{ji} = S_i$$

$$G(ID_i) = S_i$$

Let $H(x) = F(x) - G(x)$, we will know that $H(x)$ is a polynomial with $k-1$ as its highest power. For $1 \leq i \leq k$, $H(ID_i) = 0$, hence $H(x) \equiv 0$, i.e. $F(x) = G(x)$. Hence, the Lagrange interpolation polynomial for a secret-sharing scheme among k members is the secret sharing polynomial. Calculate $F(0) = G(0) = \sum_{i=1}^n f_i(0) = SK$

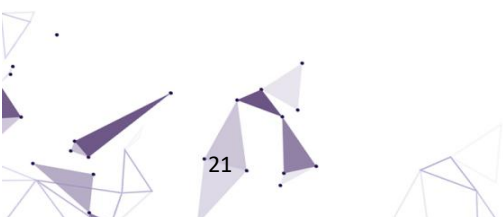
(b) Proof of Security

$F(x) = \sum_{i=1}^n f_i(x)$ is a polynomial with the highest power of $t-1$, with t number of coefficients. However, when $k < t$, only equations can be formed. From linear algebra theorem, we know that when the number of equations is less than the number of unknowns, the system has infinitely many solutions. In this case, it is impossible to determine the coefficients of the polynomial, and consequently unable to determine $F(x)$. Therefore, when $k < t$, we are unable to ascertain any information about the initial secret SK.

When the number of nodes in the network (including new group members) received the same new group public key reaches threshold t , the new group is considered successfully established. The public key is true and will be written on local group chain.

5. Asynchronous Group Building

Whenever a new group is created, the parent group has to come up with a list of candidates for the new group and send it to the new group members. The new group members will decide among themselves on the creation of the group private key. The process of creating a new group and applying to join the group are conducted asynchronously. From the above illustration, when





creating a new working group, all members are required to send their secret packet at the same time. But in reality, this condition is easily compromised. As long as one member is offline, the group building process cannot proceed, which significantly hinders the probability of successful formation of the group. To solve this problem, the Chiron consensus supports asynchronous group creation through engineering design. Fault tolerance is designed to accommodate members going offline when new group is created. As long as these members come online within the stipulated period and discover that they have been assigned to a new group, Step 1 and 2 of the group creation process will be automatically triggered so that the member will share his secret packet with the other group members. Upon receiving the secret packet, the other members will feedback by sending their secret packets to the member. By asynchronously collecting all the shared secret packets within the group, a new group can be successfully established.

2.1.3.2 Block Chain model

1. The Data Structure of Blocks

- BlockHeader: the information of the block head
- Hash: hash of the current block
- Height: height of the current block
- CurTime: time taken to generate a block in the current block
- PreHash: the hash of the previous block
- PreTime: the time taken to generate a block in the previous block
- Castor: Proposer ID
- GroupID: Working group ID
- Signature: random number
- Transaction []: transaction set with a list of hash
- Nonce

2. Shamir's Secret Sharing Scheme Incorporating ECDLP

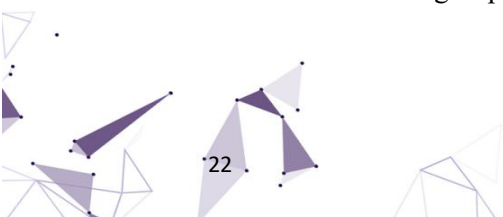
We will use Barreto-Naehrig curves $E: y^2 = x^3 + ax + b \in GF(p)$, in which finite prime field $GF(p)$:

$$p = 36x^4 + 36x^3 + 24x^2 + 6x + 1$$

$$p = 36x^4 + 36x^3 + 18x^2 + 6x + 1$$

Where x is a 63-bit number, and p and r are prime numbers with length of about 256-bit.

Two finite groups:





$$G_1 = E(GF(p))[r]$$

$$G_2 = E[r] \cap Ker(\pi_p - |p|)$$

We will use the optimal linear pairing operator on a Barreto-Naehrig elliptic curve found in recent studies, and define $e: G_1 \times G_2 \rightarrow GF(p^{12})$ as:

$$e(Q, P) = (f_{6x+2}(P) \cdot H)^{(p^{12}-1)/r}$$

Here $H = l_{Q_3-Q_1}(P) \cdot l_{Q_1-Q_2+Q_3}[6x+2]Q(P) f_{6x+2,Q}(P)$, can be calculated using Miller-Rabin primality test.

Based on the characteristics of bilinear operator: for any $P_1, P_2 \in G_1, Q \in G_2$, there exists $e(P_1 + P_2, Q) = e(P_1, Q) e(P_2, Q)$; for any $P_1 \in G_1, Q_1, Q_2 \in G_2$, there exists $e(P_1, Q_1 + Q_2) = e(P_1, Q_1) e(P_1, Q_2)$; for any $P \in G_1, Q \in G_2, a, b \in Z$, there exists $e([a]P, [b]Q) = e(P \cdot Q)^{ab}$

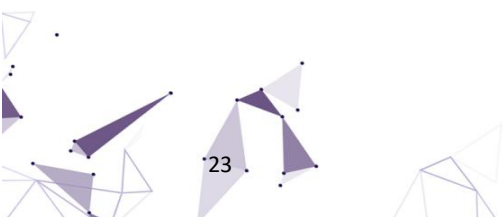
Here, we use $[.]$ to denote multiplication on elliptic curves. For example, $[a]P$ denotes the a-times multiplication of point P on the elliptic curve. based on the elliptic curve digital signature algorithm:

- $m \in \{0,1\}^*$: secret that needs to be signed (in binary)
- Compute $R = H(m) \in G_1$
- Compute $\sigma = [x]R$, where x is the private key of user signature, σ is the signature obtained.

Combining with the aforementioned group construction (decentralized Shamir's secret sharing), we establish a correlation between member signature private key S_i and group private key SK as follows:

$$SK = \sum_{i=1}^k S_i \prod_{j=1, j \neq i}^k \frac{x-ID_j}{ID_i-ID_j}, \text{ where } k \geq t$$

Hence, for secret $m \in \{0,1\}^*$, the member signature is $V_i = [S_i]R$, from the characteristics of binary elliptic curve, we can obtain the following equation.





$$[SK]R = [\sum_{i=1}^k S_i \prod_{j=1, j \neq i}^k \frac{x-ID_j}{ID_i-ID_j}]R = \sum_{i=1}^k \prod_{j=1, j \neq i}^k \frac{x-ID_j}{ID_i-ID_j} V_i$$

In other words, on bilinear elliptic curves, after signing the information with all members' signature private keys obtained from the above grouping method, we get kt signed secrets, and we can use the Lagrange interpolation polynomial to obtain the secret signed by group private key SK.

In Shamir's secret sharing algorithm, S_i must be revealed in order to reconstruct group private key SK. Using bilinear mapping of the properties of e , the signature of group private key can be obtained without compromising S_i . This renders group private key recyclable for repeated uses. Through this technique, group consensus can be achieved by threshold signatures. The process is more efficient than Byzantine fault tolerance (BFT).

3. Group Collaborative VRF Random Number

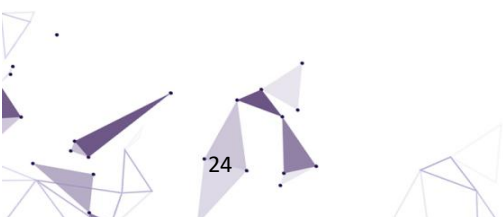
As no one knows the group private key SK, the signature $[SK]R$ is non-selectable, unpredictable and immutable, but it can be verified by the group public key gpk to ascertain whether it is signed collectively by the group. It is a technique to generate group collaborative VRF random numbers.

The method Chiron uses to generate random numbers is the aforementioned group collaborative VRF technique. Let $B^r.Rand$ be the Rand value of the block generated in the i^{th} round slot. We use random number

$$R_r = \text{hash}(B^{r-1}.Rand) \text{ for the } r^{th} \text{ round slot.}$$

Using group selection strategy, the working group for the r^{th} round slot can be determined. The current working group pairs sign and collect signatures that are equal or greater than the threshold value. The reconstructed group private key pair $(r|R_r)$ will be used as randomly generated number of the current slot and written into the $B^r.Rand$ of the block generated in the r^{th} slot.

$$B^r.Rand = \text{recover}(\text{sig}_1(r|R_r), \text{sig}_2(r|R_r), \text{sig}_3(r|R_r), \dots, \text{sig}_t(r|R_r))$$





The Rand of the previous block determines the current working group. The current group calculates Rand of the current slot with the formula above to determine the next block. RR is the Rand of the genesis block, and it is set during the initiation of the system. If in the r^{th} round, the working group is unsuccessful in generating a block, in the $(r+1)^{th}$ round the random number is determined by the following equation.

$$R_{r+1} = \text{hash}(\text{hash}(B^{r-1}.\text{Rand}))$$

Using the group selection strategy, we can determine the working group of the $(r+1)^{th}$ slot to carry out the threshold signature on $r+1|R_{r+1}.\text{Rand}$ for the current block will subsequently generated. If there is still no block generated in the $(r+1)^{th}$ round, Rand for the next round will be generated from the Rand of the current block. The process goes on.

4. Validation Group Selection Strategy

Suppose we are currently entering the r^{th} round slot, calculate the current epoch

$$e = r/\text{epoSlots}$$

Random number $R_r = \text{hash}(B^{r-1}.\text{Rand})$, and we can get the current working group list gB from the group chain

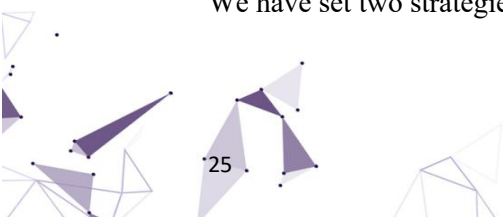
$$gB^i | gB^i.\text{GIS}.\text{Activation } e < gB^i.\text{GIS}.\text{Deactivation}$$

Using the random number R_r as a random seed, the pseudo-random number generation function PRG can be used to randomly determine the current working group in the above existing working group list gB. These choices are auditable and verifiable by other nodes. In the later development stages, we may consider taking the group's health index (the sum of group member health indexes) and use the Follow-The-Satoshi (FTS) algorithm as the basis of group selection.

2.1.4 Convergence Optimization and Communication Optimization

Due to the dynamic size of the proposal group, multiple candidate blocks may be generated at the same time. Therefore, the algorithm must quickly converge on the candidate block.

We have set two strategies:



- The validation group will give priority to the proposal group to obtain the information of the validated block in the previous round (the block that completes the group signature. Multiple block may exist). In addition, the validation group will give priority to process the weight of the blocks of the previous round;
- As the validation group is preparing to sign, when a candidate block reached a group consensus and is broadcasted, no other candidate blocks of the current round will be signed.

With reference to the propagation performance of Bitcoin's P2P network, it takes 1 second to complete a transmission of a 1KB message to 95% of the network, whereas it takes 1.5 minutes to complete the transmission of a 1MB message to 95% of the network transmission. We must also take into account that the group members are scattered around the world, and the working group will propose multiple blocks as candidate block. Therefore, it is imperative to optimize communication accordingly. We consider adopting Block header within the group to communicate with the validation group. As the group reaches strong consistency on the hash of block header, it only guarantees the content of the block and the time sequence. The existence of double-spending in user accounts cannot be verified. Therefore, after rapidly reaching strong consistency on the hash, the transactions are synchronized locally. The validation of the account status on chain will ensure the validity of the transactions. With this process, a higher consensus can be achieved. If the proposing miners are honest, the workflow is more efficient than the classic way of information transmission, which mobilizes the entire blockchain, including all transactional information on block. If the proposing miners are malicious, validation will fail when the block come on chain. Validation outside the group is prohibited from broadcasting, thereby ensuring security. In addition, if a proposal miner is malicious, the bonus contract is immediately called after the verification group validates the transaction. But failure in new block validation will render the block fail to come on chain. The bonus contract called will be inconsistent with the one on block, acting as a solid proof of malicious activities. Corresponding punishment will be carried out on the miner, such as forfeiture of deposit or deduction in health index of the miner.

2.1.5 Forking

1. The Decision to Fork

Due to the characteristics of the consensus mechanism and the uncertainty of the P2P network, soft forks are inevitable on the blockchain. Upon the occurrence of a soft fork, the nodes on ZV

CHAIN will prioritize the fork $totalG = \sum G_i$, where G_i is the priority level of each block as shown in Figure 2.4.

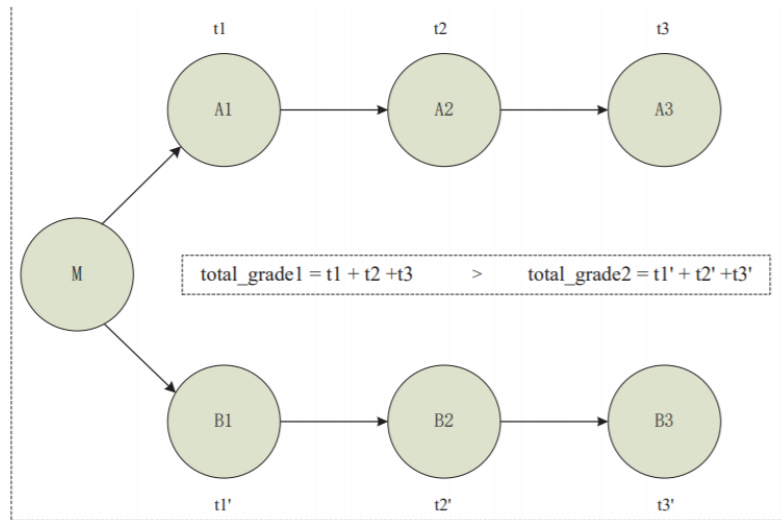


Figure 2.4: Schematic Diagram of Chiron Forking

As a specification chain, the forking nodes will quickly and easily adjust local chains to specification chain through forking adjustment, thereby ensuring consistency on the regular chain.

2. Forking Adjustments

A node locates the forking point first when it undergoes forking. It will then make a selection by comparing the total priority from the forking point to its current height. In the process of searching for forking points, a regional search mechanism will be employed to conduct a binary comparison on target chain segments of a certain step size. The step size will be adjusted according to the results of the comparison, so that the forking points can be quickly located to carry out forking adjustments.

2.1.6 Checkpoint Mechanism

Finality, broadly defined, refers to specific operations that once completed will be chiseled permanently and irreversibly in history. This is a crucial concept in the financial industry. ZV CHAIN is a public chain that undertakes banking services and data certainty is a central security factor that must not be overlooked. The final consensus of the data will be confirmed with finality and not with probability, unlike the 6-block confirmation used by Bitcoin.

The Chiron consensus provides a periodic checkpoint mechanism. The cycle for the checkpoint is the epoch (the preset epoch cycle by the system. For instance, the system can set its default epoch to the duration of 100 blocks). According to the Chiron grouping mechanism as mentioned above, the number of validation groups is fixed during each epoch cycle. An algorithm similar to the Hashgraph is used to find a "strong" visible connection (in essence trying to achieve a Byzantine fault tolerance with an endorsement from at least two-thirds of its members), and to determine the status of the “checkpoint” with the information on hand.

The checkpoint mechanism, assuming that the current block height enters the $(n+2)^{th}$ epoch cycle, will backtrack to the n^{th} epoch and find in the interval any sub-chain block that has obtained validation from two-thirds of the groups in the validation group set. Chiron’s checkpoint mechanism, unlike DAG or Hashgraph, will be able to predict the finality time as every slot has a unique, random and unpredictable validation group in charge of the validation process, proven in the section of VRF group selection. In other words, the probability of a group being appointed the task of verification is equal, therefore in each epoch, finding a sub-chain with two thirds endorsement is common and highly probable. The final blockchain of ZV CHAIN can prevent long-range attacks. Even if 51% or more nodes in the network is being controlled, any attempt rewrite history outside the latest checkpoint will be stopped.

2.1.7 Consensus Analysis and System Security

We consider a system highly-secured if the solutions proposed to counter security breaches such as double spend attacks, long-range attacks (private mining), nothing-at-stake attacks, sybil attacks, and 51% attacks are proven through mathematics or game theories. Fundamentally, all attacks can be roughly boiled down to the four attacks as stated above. These attacks can precipitate temporary or permanent damage to the system and individuals. The periodic Checkpoint mechanism illustrated above guarantees the finality of blockchain data on ZV CHAIN. Even if the attacker controls more than 51% of the nodes, the attempt to override transaction history outside the latest checkpoint will be curbed. Therefore, attackers with more than half of the nodes under their control can only modify recent blocks, i.e. blocks between the current block and the latest checkpoint. Apart from the checkpoint mechanism, ZV CHAIN also offers a monitoring system against the most severe 51% attack by introducing the concept of system health indicator, which helps users get a better idea of the system condition at one glance, and safeguards security by suspending or delaying the final confirmation block of the transaction.



2.1.7.1 Consensus analysis

1. Decentralized analysis

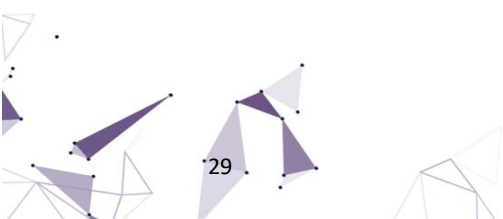
The PoW consensus is a highly decentralized algorithm. However, as mining hardware and mining pools have become more prevalent, they are emerging as the hidden center of the PoW consensus. It is almost impossible for participants using hardware with mediocre hashing power to gain profit from mining activities. The Chiron consensus divides nodes into heavy nodes and light nodes. Heavy nodes obtain the right of proposal through VRF random secret balloting. The probability of obtaining the right of proposal is linearly correlated to the staking amount for a single heavy node. In contrast, light nodes are randomly grouped, and the actual working group is determined by true random number in a particular round, thus making sure that all groups have equal chance of becoming the validation group. The proposer of the final block, together with group members who are involved in the validation process, is rewarded for block generation.

2. Consistency and Accuracy Analysis

Chiron designs a checkpoint mechanism with one CP per 100 blocks (about 5 minutes). A consistency check is done during the validation stage of block generation, while an accuracy check is done during the proposal and block generation stage. When the non-block generating groups in the full network receive a new block, they will conduct an accuracy check on the content of the block. If any issues surface, a voting session is carried out within the group. If more than threshold number of votes agrees that the block has problem, then voting will be done with every group as a unit to a specialized smart contract. The voting nodes share the benefits and the penalties of the vote. At the beginning of every new CP, the smart contract should be checked. If more than N groups have voted for abnormality in block generation of the previous CP, then an accuracy check shall be carried out. If the abnormality is confirmed, then the process backtracks to the previous CP and restarts. Otherwise it will proceed with the current CP. For most small and medium-sized transactions, they can be confirmed once 90% of neighbor nodes are observed to generate three additional consistent blocks after the block containing the transaction information. For large transactions, we suggest confirming the transaction once 90% of the neighbor nodes have entered a new CP.

2.1.7.2 System Security Analysis- Defense Against Attacks

- Nothing at Stake Attack



In pure PoS algorithm, incentives are given to reward block generation, but there is no penalty for malicious block generation or forking due to errors. As a result, under the condition of intense multi-chain competition, the best strategy for rational miners is to mine on every single chain. By employing this mechanism, the miners will receive rewards regardless of which chain triumphs. As the hashing power invested is virtually negligible, the winning miners are able to maximize their gains with extremely low costs, as shown in Figure. 2.5.

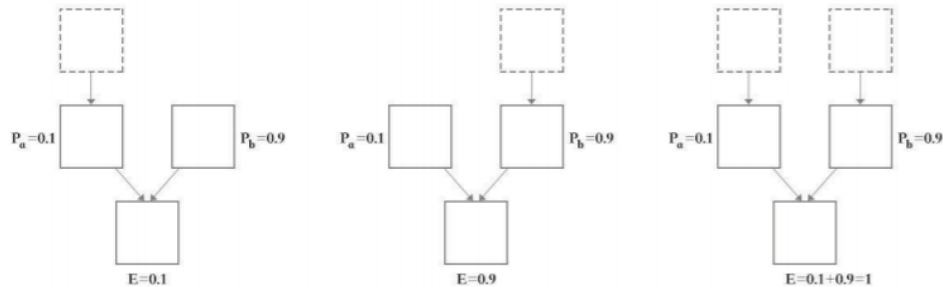


Figure 2.5: Schematics of Nothing-at-Stake attack

P_a and P_b are the winning probabilities of two forks respectively. When miners vote on both forks, E (the expectation of returns) is maximized. In extreme cases where all miners on the network are profit-driven, no consensus will be reached even in the absence of attackers.

In a traditional PoW algorithm, all miners engage in a real-time competition of hashing power. In order to implement a Nothing-at-Stake attack, the miners must distribute their hashing power into two branches, which will greatly hinder their competitiveness. Therefore, the traditional PoW is naturally resistant to Nothing-at-Stake attacks.

In fact, in the Chiron system, VRF selects a corresponding working group at each block height. This ensures that among multiple branches, only one block that has the right to generate blocks in each round. Similarly, there is only one share of revenue. Therefore, other non-block-generating groups are not economically driven to maintain two forks. They will opt to make a choice between the two forks and reach a consensus eventually. In addition, the block proposer and verifier need to call upon the bonus contract after the block is generated to receive their rewards. The system sets penalty on multi-block generation at the same block height. When irregularities in calling the bonus contract during multiple block generation is detected by the miner in charge, it will then be submitted as evidence of malpractice.



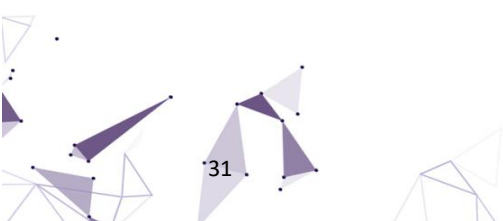
The system will in turn punish the block generator at that height, thus we believe that the Chiron algorithm eliminates the problem of nothing-at-stake attacks.

- Sybil attack

One form of sybil attack is when the attacker creates a large number of pseudonymous identities and uses them to gain a disproportionately large influence and to increase his own profits from mining. ZV CHAIN mobilizes the traditional rights staking mode to facilitate block generation as the proposal probability on heavy nodes is linearly correlated to the staked right. Therefore, distributing the right to multiple accounts to participate in block generation is not going to improve the expected returns. Similarly, the probability of a light node being selected is also linearly related to its staking rights, thus it is not lucrative or economically viable to perform a sybil attack.

Another form of sybil attack involves the attacker interacting with honest miners and stealing their benefit through certain means. In the ZV CHAIN system, there are three types of interaction among nodes, namely one-way, two-way and cross-chain interaction. One-way interaction refers to receiving and storing information after its legitimacy is validated, such as data synchronization messages. Owing to a unidirectional communication, the attacker is not able to gain any profits from this type of interaction alone. Two-way interaction refers to receiving information and giving feedback to the sender (or other group members) after the information is validated, such as the block validation messages and group creation message. The attacker can camouflage as a group member and establish communication with the victim during group building or the validation process in an attempt to steal profit. As the group creation process is initiated by the designated parent group, the selection of founding members is performed by obtaining node signatures that exceed the threshold value from the parent group, thus it remains auditable and immutable. Real group members can be easily distinguished from the imposters. Cross-chain interaction refers to receiving and transferring information, which apparently will not benefit the attacker. It is noteworthy that the attacks mentioned above are rendered futile with the assumption that the miners' private keys are not disclosed, as all interactions on ZV CHAIN do not involve the transfer of private keys.

In conclusion, the ZV CHAIN system prevents malicious attacks with a self-improving feedback mechanism consisting of block generation participation and system health index. A





secure and verifiable communication mechanism eliminates any possibility of security breach and profit theft that cause damage to users' interests.

- 51% Attack

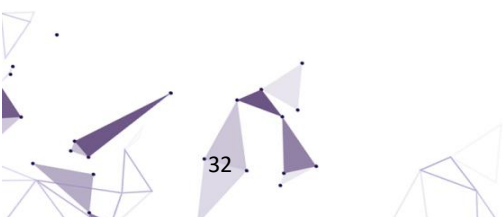
In pure PoW systems, the adversaries of 51 percent attacks are fatal and irreversible, because the attackers have sufficient hashing power to branch out a longer and more complex chain to eliminate the main chain. Honest miners will gradually accept the attacker chain, the attacker will henceforth emerge victorious. The ZV CHAIN system randomly assigns miners to different groups. 51% of the attacks may result in attackers controlling most of the working groups. In this case, the main chain will be extended slowly, and the attacker chain will be extended more rapidly because it controls more groups, and the chain will keep increasing as long as honest miners reject the attacker chain. At this time, the vast majority of users can easily perceive that there are two different chains in the system, and they are thus afraid to trade rashly. This in turn generates little profit that is utterly disproportionate to the cost of initiating a 51% attack.

If all nodes that are randomly connected to an ordinary user are controlled by the attacker, the user will continue to trust the network because he cannot perceive any anomalies in the system. We believe that these users can bring benefits to the attacker, and we shall address them as “victimized users” for the time being. Apparently, the more victimized users, the greater the benefits of the attacker. The following is a brief analysis of the proportion of attackers and victimized users.

Assume that 90% of the n nodes randomly connected to each user are controlled by an attacker, rendering the user a victim. Assume that the number of nodes in the entire network is W and the attacker control ratio is x , the victim ratio is:

$$V = \frac{\sum_{i \geq 0.9n} \left(\frac{(W \cdot x)}{i} \right) \left(\frac{W \cdot (1-x)}{n-i} \right)}{\left(\frac{W}{n} \right)} i \in N$$

More generally, let $W = 10000$, $n = 10$, the curve of v and x is shown in Figure 2.6 below.



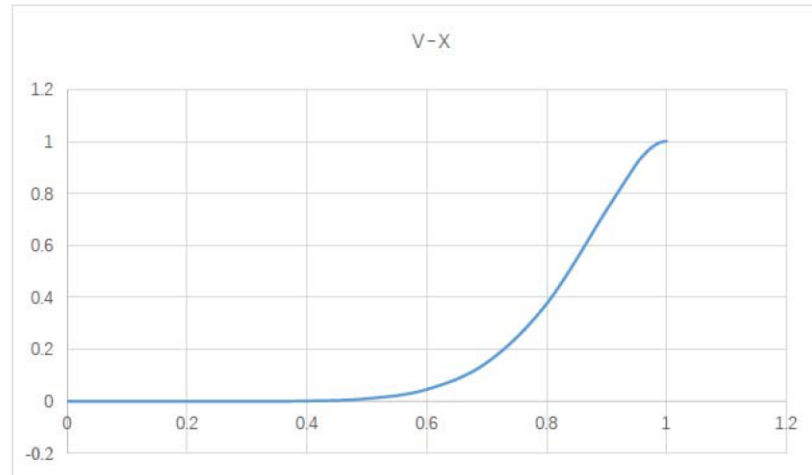


Figure 2.6: Relation Between the Ratio of Attackers and Victims

From the graph above, we know that when the attacker controls 50% of the nodes, the percentage of victims is only 1.07%. Theoretically, the attacker can dominate the network only if he controls 100% of the nodes. If the percentage of victims exceeds 90%, the attack is profitable, but the attacker should control more than 95% of the nodes. The cost of attack is enormous.

Table 2.2: Key Points of Comparison

0.5	0.01071
0.8	0.3757
0.9	0.7361
0.95	0.914
1	1

Conversely, when the attacker withdraws due to unprofitability, the system will restore if the percentage of honest miners is more than 95%.

ZV CHAIN is unlikely to be susceptible to the 51% attacks that have been plaguing low hash-power PoW public chains as its system will be able to resist attacks higher than 95% with the initiation of



further improvement to the health threshold of the system during cold start or in low power states. As a result, ZV CHAIN will be able to offer a higher level of security.

- Long-range attack

Under the PoS algorithm, there are no limits imposed on the speed of block generation. During the early stages, there is not a large number of miners. If these miners unite and revert to the initial stage of the system to generate blocks, they would be able to create a longer chain within a shorter span of time. Presently, ordinary users cannot distinguish the main chain from the attacker chain, and it is probable that the attacker chain may triumph over the main chain. At present, many PoS implementations attempt to increase the difficulty of attacks by limiting the number of rollbacks.

In the ZV CHAIN system, the upper and the lower limits of block difficulty are set to be D_{max} and D_{min} , and $D_{max} = k \cdot D_{min}$. with the H_{epoch} denoting the width of each epoch. The working cycle of each working group consists of n epochs. At the end of each working cycle, the group will be automatically dismantled, and subsequently enters the reconstruction stage. Assuming that the attacker chooses to revert to H block to initiate a long-range attack, and that the ratio of groups controlled by the attacker is x , owing to the randomness of VRF, the attacker can only generate blocks during the selected window period, while churning out empty blocks during the non-selected window periods. In the long run, the ratio of effective blocks in the attacker chain is directly proportional to the percentage of groups controlled by the attacker. After n epochs, the status of the chain is shown in Figure 2.7 below.

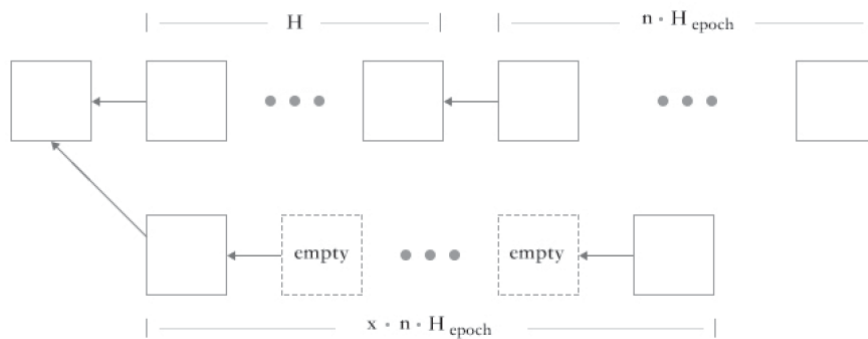
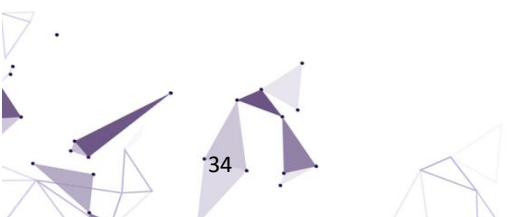


Figure 2.7: Schematic of a long-range attack

Table 2.3: Minimum Percentage of Groups that Attackers Should Control



K value	The range of x
1	Greater than no solution
2	Greater than 50%
3	Greater than 33%
5	Greater than 20%

The maximum cumulative chain difficulty that an attacker can compute in a working cycle is as follows:

$$D_{attack} = x \cdot n \cdot H_{epoch} \cdot D_{max} = x \cdot n \cdot H_{epoch} \cdot k \cdot D_{max}$$

Then, the minimum cumulative difficulty of the main chain is:

$$D_{main} = (H + n \cdot H_{epoch}) \cdot D_{min}$$

The conditions for an attacker to succeed is:

$$D_{attack} > D_{main}$$

After simplification:

$$n \cdot H_{epoch} \cdot (k \cdot x - 1) > H$$

Thus, the attacker can only revert to a limited height to carry out long-range attacks. When $k \cdot x \leq 1$, the probability of a successful attack will be 0. This means that the attacker must control more groups to reduce the difficulty of an attack. Table 2.3 shows the minimum percentage of groups to be controlled for different K values.

In fact, stringent conditions must be fulfilled for deductive reasoning to hold true. Firstly, all groups controlled by the attacker must be in the same life cycle in order to sustain the attacking power. This condition is difficult to achieve in a random group-building model. Secondly, the deductive reasoning assumes that the attacker can reach the upper limit of the block difficulty every time, while the honest miners are barely able to reach the lower limit of the block difficulty. As long as either one of the two conditions are not satisfied, the range of H will be significantly reduced. Finally, refusing to accept outdated (n number of blocks back) blocks on the part of honest miners will limit the number of blocks to which the system can perform rollbacks on.



In short, imposing difficulty levels and the effective time of blocks limits the number of blocks the system can perform rollbacks on while random grouping strategy and group periodic reconstruction mechanism make it impossible for the attacker to maintain a long-term, high-intensity attack. This makes it almost impossible for the ZV CHAIN system to suffer long-range attacks.

- DDOS attacks

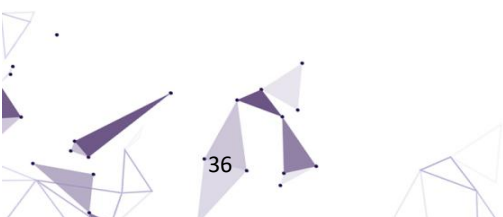
DDOS attack refers to attacks initiated by perpetrators who organize a batch of computers to submit a large number of requests to service nodes aiming at exhausting resources by keeping the service nodes busy processing requests, to the extent that the nodes are unable to continue providing services. All nodes in the Bitcoin and Ethernet network engage in decentralized PoW computation. We believe that the degree of decentralization will determine the strength of defense against DDOS attacks. The Chiron algorithm uses VRF to randomly select validating groups across the network. On the surface, the validating group becomes the temporary center of the system. However, owing to the randomness and unpredictability of the VRF mechanism, the “virtual center” changes dynamically each round, so fundamentally the system remains decentralized.

- The Last Member Attack

All nodes in the ZV CHAIN system participate in the distributed ledger through group collaboration. Every block is validated by the threshold signature, and nodes outside the group can be validated with the group public key. As such, it is immutable. If the last member attempts to manipulate the data, it will ultimately result in a failure in validation with the attacker left with nothing to gain. Deliberately remaining inactive is also a form of last-member-attack. However, in ZV CHAIN, any node within the group can be the last member, so a single point does not exist. As long as an honest node exists, the attacker is deemed to fail. Under extreme circumstances where the attacker controls all members in a certain group, a veto by the attacker will trigger the system into skipping the current round and proceeding directly to the next round, rendering the attack futile.

- Double Spending attack

The common practice of a double-spending attack is to create a sub-chain that can potentially take over the main chain. The attacker needs to control at least half of the nodes in a certain group to initiate an attack. In order for this to happen, the attacker broadcasts his transactions whilst a





block is being generated, before transferring the transaction to a different fork. This will happen simultaneously with the generation of a new block on the same fork. After the transaction is confirmed on the main chain (the confirmation time is short), the attacker then broadcasts the fork. If the difficulty of the forked chain is greater than the cumulative difficulty of the current main chain, the attacker chain will gain recognition as the main chain. Records of the previous transaction will disappear as if they have never existed. This attack strategy is similar to that of long-range attacks. For detailed explanations, please refer to the section on defense against long-range attacks.

- **Private-mining Attack**

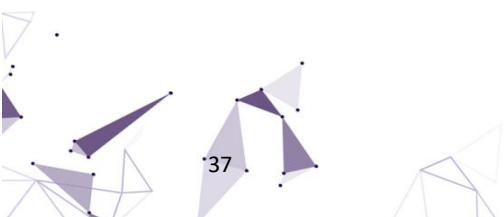
In the bitcoin system, all miners can perform PoW mining at any block height. Nodes with a stronger hashing power can hide the blocks they have mined and embark on the next mining cycle discreetly to get a head start. In ZV CHAIN, all miners mine collaboratively in groups. In order to broadcast a generated block, the miner needs to gather threshold signature from majority of the group members, rendering private mining impossible for individual miners. On a group level, the group is not guaranteed the right to mine as group rotation is solely based on VRF. As a result, privately mining is also impossible for group collusions.

The single chain performance of the Chiron consensus mechanism is 3000 TPS, a rate that sets the stage for high-level security and decentralization. Chiron offers the optimal solution to the impossible trinity of decentralization, security and performance as compared to all existing consensus mechanisms. The Chiron consensus mechanism has considered the issue of cost-effectiveness in performance since the conception of the project and capitalizes fully on group idle time as well as the design of the periodic checkpoint mechanism.

2.2 Privacy-Preserving Computing and Security Framework

2.2.1 Data Privacy and Regulation

The key features of the blockchain technology include decentralization and credibility, both of which enables reliable P2P value transfer amongst unknown nodes without relying on a trusted third-party authority. These key features are instrumental in reducing transaction costs and enhancing the efficiency of interactions. The blockchain technology has broad applications in the future with an optimistic outlook and is believed to be the pivotal technology in leading the transition of the Internet from an information





network to a value network. However, with the development and application of the blockchain technology, the problem of data security has become increasingly pronounced.

1. Transaction privacy

Bitcoin, the creative brainchild of Nakamoto Satoshi and the decentralized platform subsequently developed, have lifted the heavy reliance on third-party transaction platforms. Yet, at the same time, all transaction records of Bitcoin must be broadcasted on the blockchain, and group consensus must be reached to safeguard the security of the entire system. In other words, in addition to the transparency of all online transaction records, the sender and receiver addresses used during transactions will be exposed. The original Bitcoin protocol does not provide extra measures to protect user privacy. After analyzing the transaction pattern of a certain address and corroborating it with real-life information, the attacker can easily discern relations between the transaction address and the actual person, which poses a great threat to user privacy. In view of these pertinent issues, researchers have proposed two fundamental attributes of cryptocurrency privacy.

a) Unlinkability

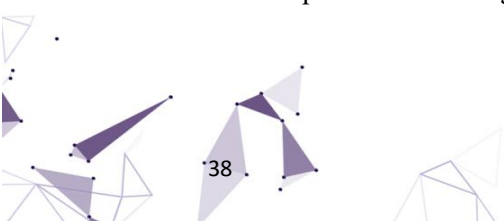
The inability to distinguish whether two transactions are sent to the same person leads to the inability to discern who the receiver is.

b) Untraceability

Untraceability refers to the inability to discern who the sender is. ZV CHAIN is a public chain that facilitates banking services; thus, data privacy protection is of utmost importance.

2. Privacy Protection Theory

We deploy zero-knowledge-proof technology to safeguard account security and user privacy. In addition, homomorphic encryption technology is incorporated in the field of data storage security and privacy protection. Homomorphic encryption is a form of encryption, which allows for computation on ciphertexts, generating an encrypted result which, when decrypted, matches the result of the operations as if they had been performed on the plaintext. From the standpoint of abstract algebra, this method preserves the homomorphism of the encrypted text. Homomorphic encryption veils the original information from the processor's gaze. It also provides a contingency plan which integrates blockchain technology with the existing infrastructure. By adopting





homomorphic encryption for data storage on the blockchain, a perfect balance is achieved, ensuring that no major changes are made to the fundamental structure of the blockchain. The blockchain remains a public chain, though on-chain data is encrypted to address the problem of privacy violation. The homomorphic encryption not only installs private chain features on the public chain and safeguards user privacy, it also allows access to on-chain data for auditing and other purposes. In other words, incorporating homomorphic encryption combines the strengths of both public and private chains. Beyond that, homomorphic encryption will allow smart contracts on the blockchain to process ciphertexts, ensuring that the original content of the contracts remain concealed which in turn enhances the security and privacy of the network.

3. Privacy Protection Schemes

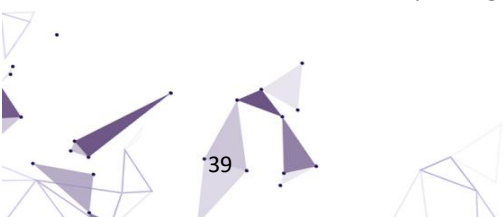
a) The Dandelion Protocol


One of the major challenges to privacy concerns in cryptocurrency is that transactions can be traced when transactions are added to mempool, transmitted across the network and linked back to the original IP address. Even on networks with effective privacy measures, the transaction information can be de-anonymized to reveal the identity of the users. The Dandelion Protocol is proposed as a network layer solution to ameliorate privacy concerns during transmissions on network. Under this protocol, a transaction is transmitted in two phases, namely the anonymity phase and the spreading phase. In the anonymity phase, transactions are relayed through a privacy graph to a single random peer, who relays to another single peer through the same algorithm. This pattern continues until one of the nodes broadcasts the transaction in the typical format of diffusion to the rest of the network, hence marking the transition into the second phase. By relaying the transaction to random peer nodes on the network before diffusing to the rest of the network, the source of transaction would become virtually untraceable.

b) I2P Anonymous Network

I2P is an anonymous network project implemented as a Mix Network. I2P is a network layer consisting of I2P routers with garlic routing, which provides a secure and anonymous platform for applications to communicate without any restrictions. I2P uses UDP and TCP protocols simultaneously and supports UPnP mapping.

To cater to the needs of Tor anonymous network users, ZV CHAIN offers support by using the SOCKET VPN to link to local Tor portals. At later stages, users will also be





able to implement orchid library on nodes or in their wallets. In addition, I2P, chosen as one of ZV CHAIN's anonymity network support, will set the stage for the implementation of local VPN or SAM implants. ZV CHAIN uses I2P's original tool to dock into the anonymous network and guarantees the anonymity of the users' network so that their IP addresses remain untraceable. ZV CHAIN has plans to employ a more sophisticated P2P network technology in the second phase of development.

c) MimbleWimble Protocol

The MimbleWimble number [10] is initially conceived as an improvement to the Bitcoin network. The transaction address and amount are concealed in the MimbleWimble protocol, while the intermediate steps are “cut-through”. During each transaction, the parties involved create a public multi-signature key. There is no address input into the system as both parties share a so-called “blinding factor” - a type of digital currency encryption which shares secrets with the two parties involved exclusively and is able to safeguard network privacy.

The MimbleWimble protocol uses the Pederson Commitment Scheme, in which full nodes deduct the encrypted amounts from both the inputs and outputs, creating a balanced equation by introducing the blinding factor that proves that no coins were produced out of thin air. During this process, the actual amount of the transaction remains unknown to the node. A “Cut-through” can be understood with the following analogy: A gives B an amount of money, which in turn is given to C in full. This is equivalent to B not participating in the transaction; thus, B's information is not recorded on the chain. Cut-through compresses the size of the blockchain, making it much lighter in terms of data storage. ZV CHAIN fully embraces regulations by providing an auditable wallet that is open to multiple auditing functions. The wallet generates an additional public/private key pair, which is used to label transactions. Auditing agencies with the public key can decrypt the transactions on the chain but are not able to create labelled transactions. This mechanism provides transparent transaction information to the authorized parties without compromising the privacy of the companies involved in the transaction.



2.2.2 Formal Proof

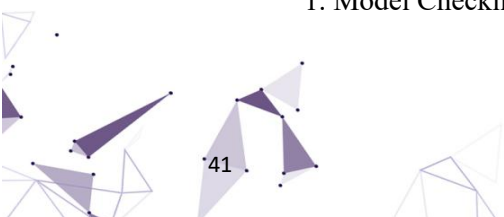
The Ethereum network brings smart contract to blockchain technology and expands the functions of the blockchain exponentially. However, just this year alone, several ERC-based ICO projects were hacked due to loopholes discovered in the smart contract codes, causing massive damage to investors. This serves as a wake-up call to all stakeholders involved in the cryptocurrency industry. Safeguarding the security of the smart contract is of paramount concern to all public chain developers. ZV CHAIN proposes the formal proof of smart contracts as a viable solution. After users upload their smart contracts, the ZV CHAIN system will carry out a validation procedure on the structure of the smart contract while incorporating the traditional “test+audit” model. The two-pronged approach is a powerful strategy to strengthen the security of the smart contract.

Currently, there are two solutions to the security issues of smart contracts, namely the testing of contract code and auditing. These two solutions will allow the detection of most security loopholes to a certain extent; therefore, they are considered necessary actions in guaranteeing contract security. However, both solutions are not without intrinsic flaws. The contract testing team develops an automatic testing software that generates an exhaustive list of test cases to verify whether the smart contract can function under various conditions. However, test cases generated are not able to cover every single scenario. As a result, even if the test results turn out to be negative, it does not necessarily mean that the contract is without security flaws. On the other hand, auditing requires the security team to assess the contract from various perspectives, such as coding, service logic etc., and provides professional opinions to the project team on how to rectify bugs. Although professional security teams are able to identify majority of the loopholes and vulnerabilities, the auditing process relies largely on the experience and judgment of the auditing team, thus it is not a 100% foolproof solution.

Formal proof is a representation of the contract code with formal logic, and strictly observes the rule of inference and mathematical deduction. This process relies on the rigour of mathematical reasoning and ensures full coverage of the runtime behaviors. The absolute correctness of runtime behaviors can be guaranteed to a certain extent. As such, the process of formal proof overcomes the limitations of the two traditional methods mentioned above.

Formal verification refers to the use of formal methods in mathematics to prove or falsify the attributes of the algorithm. There are two types of formal methods:

1. Model Checking





All possible states of the system are listed and tested exhaustively. The process is fully automatic but cannot be scaled to large systems.

2. Deductive validation

A collection of mathematical proofs is generated from the system, and it is discharged using either interactive or automatic theorem prover. This method is suitable for large systems but requires manual conversions of the operation method of the system into a language that the verification system can understand.

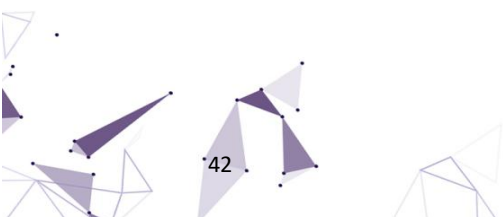
In blockchain applications, if security is compromised during the implementation of smart contracts, it will cause enormous and irreversible damage to the users, due to the immutability of the blockchain. Once the network is under attack, a group consensus must be reached in order to roll back the transaction. However, rolling back is not the most effective nor realistic remedy to malicious attacks. It is thus crucial to perform numerous trials and errors during the development stage to fend against malicious attacks. Yet, trial and error, though comprehensive, has its own trade-offs as it inevitably sacrifices the speed of iteration. The scarcity of blockchain developers renders it more challenging to keep up with the surge in the number of smart contracts developed. Moreover, the cost of manual audit is enormous, therefore the transition towards machine-aided validation is imminent. It is relatively straightforward for machines to perform syntax and semantic validation due to the low technical entry threshold. However, the machine-aided validation stops at the correction of superficial errors and is unable to comprehend deep-level programming logic. Ultimately, formal proof is the only means that has immense potential to shed light on enhancing the automated auditing process of smart contracts.

2.2.3 Communication Security

The network communication security is achieved by the logic of the application layer. At the application layer, we classify communication information across the entire network according to the security requirements. For communication that requires secure channels, we will use the ECDH encrypt secure channel for P2P communication, to bulwark communication security.

2.3 Smart Contracts

In the process of rapid DAPP development, we are confronted with similar problems that are facing traditional application development, if not more intense. These problems are the undesirable side



effects of a decentralization network. ZV CHAIN aspires to create a holistic and effective ecosystem for developers, premised on honoring the spirit of contract, safeguarding security and guaranteeing equality and fairness. The system is designed to facilitate the rapid development and implementation of DAPP projects.

2.3.1 Contract Upgrade

Functional upgrading has always been an integral part of the traditional application development process. Transaction is the precursor of DAPP. The trade-off of honoring the blockchain spirit - “code is law” is that functional upgrade has yet to gain traction with respect to systemization. ZV CHAIN ultimately envisions to build a robust commercial platform for DAPP development. We propose to establish a holistic contract upgrade and facilitate the negotiation of functional upgrade planning between the contract initiators and users on a platform level. The contract initiator sends a contract upgrade invitation to users, who upon receiving it, will evaluate the potential impact of the proposal on their individual interests, and decide if they wish to proceed with the upgrade. The process is illustrated in Figure.2.8.

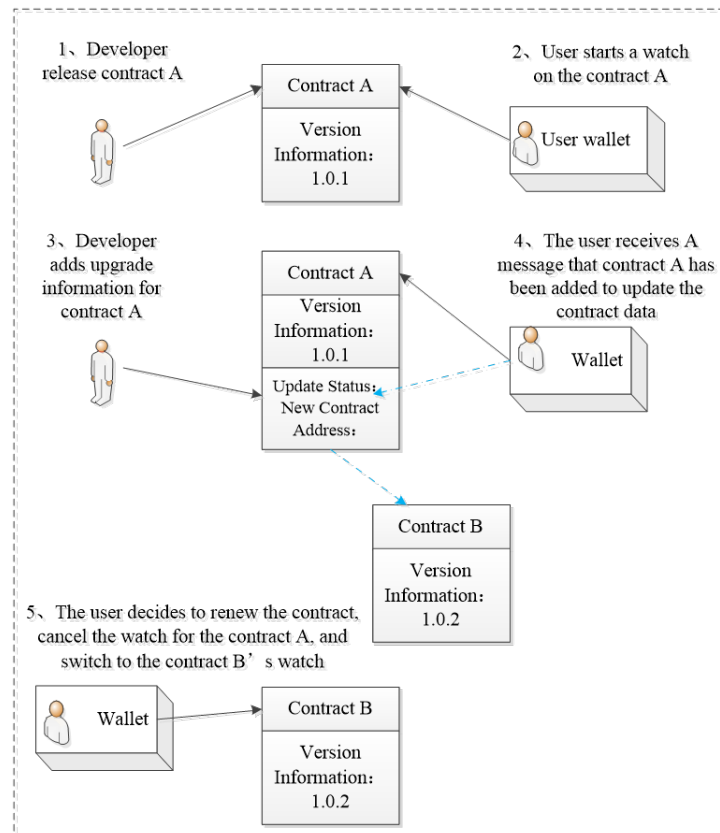


Figure 2.8: Smart Contract Upgrade Diagram



2.3.2 Major Anomaly Repair (Hard fork)

In traditional application development, in addition to daily functional upgrade and bug fixing, there are also forced upgrades triggered by major bugs and data rollbacks. During the DAPP iterations based on smart contracts, the decision of whether to enforce an upgrade or data rollback should not be decided by the developers alone. Support from the platform level is instrumental in rapidly restoring the system and solving severe problems during DAPP operation to achieve minimal hard fork.

ZV CHAIN will provide a comprehensive set of interfaces and toolchain to assist developers to swiftly proceed to fork when major bugs are detected during DAPP operations. These include mirror-duplicating the contract, data copying and rolling back to a specific height, and broadcasting to all DAPP participants.

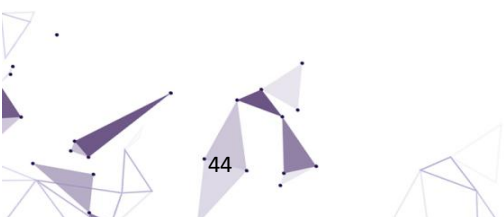
2.3.3 Efficient VM and Contract Language-Python

ZV CHAIN uses TVM which is developed in-house and supports scalable primitives as the keywords for smart contracts. It also supports several user-friendly programming languages, such as python and go, and offers a variety of smart contract templates for common scenarios, which can be called by simply changing a few settings.

Python is a highly accessible programming language, with a smooth learning curve, and can be learnt in an interactive environment powered by command-line interpreter. The syntax of Python is elegant, reflecting a minimalist thinking, while the code is exceptionally readable, with an efficient code audit; The linguistic ecology of Python is sophisticated with a comprehensive built-in library and a myriad of third-party API gateways by virtue of Python's open source feature. The strengths listed above are testimonies to Python being a highly capable development language - simple syntax and comprehensive libraries can significantly enhance the development efficiency, while the linguistic characteristics of the script lower the cost of debugging. The ease of learning renders python one of the most popular introductory language among beginners and is most widely accepted as a contract language.

2.3.4 Financial Service Standardized Component Library and Component Market

TVM introduces a series of generic component libraries that offer high efficiency and low GAS consumption. Apart from providing high decoupling function and reusability, TVM also significantly reduces the consumption of storing data on the blockchain. Calibrating frequent requests across industries, TVM will establish a standardized protocol to streamline the standardized procedure for wallets to handle requests. In the meantime, TVM will build a standardized component market to encourage the development of component libraries by the third party. Subjecting to rigorous auditing, these third-party



libraries will be stored on the blockchain, and released to DAPP developers, to further cut down the cost of research and the storage consumptions. Calling the components alone will not be charged. The platform will reward tokens to component developers according to the times their components are called. In addition, the platform prevents malicious calling by giving out tokens that are less than the GAS consumption each time. By employing the incentive mechanism, developers are motivated to take more initiatives, and component libraries substantiated which in turn ease the development of DAPP. With the proliferation of third-party libraries, developers will receive incentives in the form of tokens which encourage them to optimize and create more practical and reliable libraries. We believe that the model of creating generic component libraries and application component libraries is instrumental to build a healthy and robust ZV CHAIN ecosystem, as shown in Figure. 2.9.

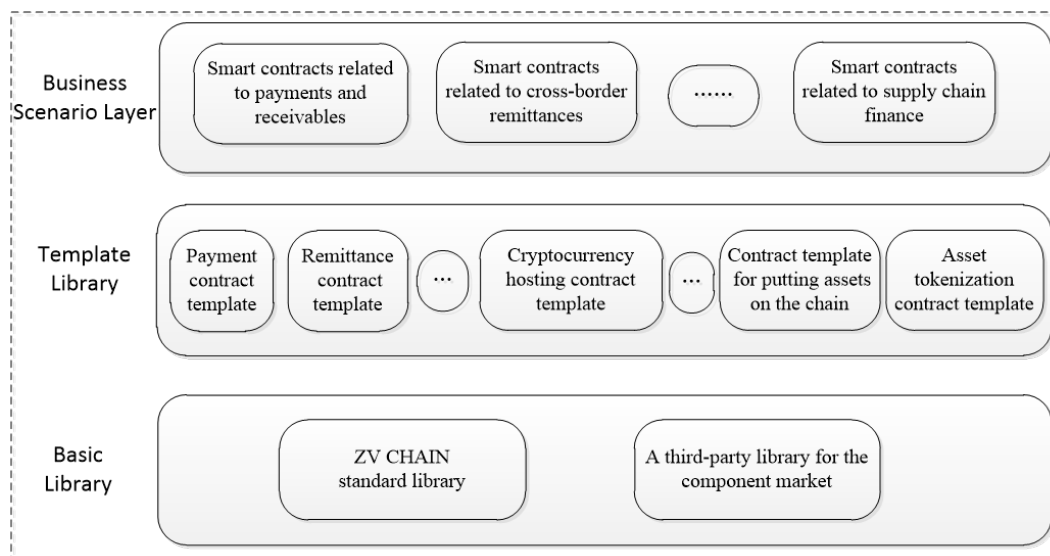


Figure 2.9: Blockchain Financial Business Standard Component Library and Component Market

2.4 Cross-chain Technology

The cross-chain technology seeks to hurdle the constraints of inter-chain operability by allowing the transmission of value and information between different blockchain network. Specifically, the blockchain network is a type of distributed ledger, with each block an independent ledger, and there is no obvious connection between two separate ledgers. Essentially, it is impossible to transfer value between ledgers. However, when it boils down to individual user level, the value stored on one blockchain by a user can be transferred to another blockchain, which in essence is the circulation of value. Currently, there

are several blockchains that are widely used, including the public chain, the private chain and the consortium blockchain. The common trend is that the development of private chain is evolving towards the consortium chain, which in turn is advancing towards the public chain. The evolution of different types of blockchain network is also a testimony to the growing demand of blockchain interoperability.

2.4.1 Major Types of Cross-chain Technology


Among many challenges facing blockchain, the lack of interoperability between blockchain networks hinders the application and potential proliferation of the blockchain. Regardless if it is public chain or private chain, cross-chain technology is the key to materialize the Internet of Value, the boat that emancipates blockchain from a deserted isle, and the bridge that connects blockchain technology to its broader applications in the outside world. In addition to the three types of mainstream cross-chain technologies mentioned in a report on blockchain interoperability [\[11\]](#) from Vitalik, the founder of Ethereum, to R3, a banking consortium, the existing cross-chain technology includes distributed private key control. All of which will be elaborated below.

1. Notary Schemes

The notary scheme has gained a lot of attention in the field of licensed ledger, as not only does it pose as a leading contestant to the scalable consensus, it also dispenses with excess Proof-of-Work algorithm, or complex proof of a benefit mechanism. Suppose there is no mutual trust established between A and B, then a third-party notary, a trusted intermediary chosen by both parties can be introduced. In that case, indirect trust is established between A and B. One of the exemplary applications of the notary scheme is the Interledger Protocol (ILP), developed by the Ripple Labs in 2002. It is not a standalone ledger nor is it seeking to achieve any consensus. On the contrary, it provides a top layer cryptographic escrow, called the “connector” or “verifier” which facilitates the flow of money between ledgers. The notary, elected by both parties involved in the transaction, is guaranteed to be highly reliable, and is to validate the effectiveness and authenticity of the data. The Interledger Protocol is applicable to all ledger systems, while the differences among which are duly accommodated. The protocol aims to establish a universal payment standard across the globe, creating a consolidated protocol for online financial transfers.

2. Sidechains/Relays

The sidechain technology facilitates asset portability between Bitcoin and other blockchain chains. It is a new blockchain technology that enables interoperability among




multiple blockchain networks by pegging the original digital assets with assets on other ledgers, not unlike the pegging of gold with fiat currency. The sidechain technology is a type of scaling technology that aims to enhance the scalability of the mainchain, and further pushes the boundaries of blockchain application and innovation. It enables the traditional blockchain network to support various types of assets, micropayment, smart contracts, security mechanisms and real-world asset registration, and enhances the privacy protection of the blockchain network. Notable Bitcoin sidechains include BTC-Relay initiated by ConsenSys, Rootstock and Element Alpha of Bitcoin's testnet, and non-Bitcoin sidechains such as Lisk and Asch.

Relays take over the task of trusted intermediaries in the notary scheme and function as channels between different chains. If the channel is a blockchain network on its own, it is then termed a relay chain. Examples of relay chains include Polkadot and Cosmos HUB, of which Polkadot plans to integrate the private chain/consortium chain into the consensus network of a public chain while retaining features such as data privacy and licensing of the original private chain/consortium chain. The mechanism of Polkadot regards other blockchain networks as parallels. During transactions, Polkadot, empowered by the relay chain technology, can temporarily lock tokens of the original chain by transferring them to a multi-signature address on the original chain. The transaction on the relay chain will be validated by the signatories through voting. Polkadot also introduces the role of fisherman who monitors transactions on the network and reports any abuses or malpractices. Polkadot connects Bitcoin and Ethereum to the Polkadot network and has the potential to render cross-chain communication a reality.

3. Hash-locking

Hash locking originates from hash time locked contract (HTLC) of the Lightning Network, which offers a scalable bitcoin micropayment channel that enhances the transaction of Bitcoin outside the Bitcoin network. The working mechanism of the key technology, HTLC, will be illustrated below. When Alice and Bob reach a commitment transaction that temporarily locks Alice's 0.1 BTC. If by time T (T refers to the future height of a particular block) Bob can present Alice with an acceptable R (known as a secret), whose hash equals the value of $H(R)$, which is agreed upon beforehand, then Bob will receive the 0.1 BTC. If Bob is unable to offer a satisfactory R value by time T , the 0.1 BTC will be unlocked and return to Alice.

4. Distributed Private Key Control



WanChain and Fusion are among the exemplary infrastructure of distributed private key control protocol. WanChain uses multi-party computation and threshold private key sharing schemes. When unregistered assets are transferred from the original chain to WanChain, the nodes of WanChain will employ an imbedded asset template based on the protocol, and establish a new smart contract based on cross-chain transaction data to create new assets on the chain. In the case of registered assets, the nodes of WanChain will release tokens of equivalent value according to the existing contract, which guarantees the transaction and circulation of the original assets on the WanChain. Parallel computing is made possible through multi-layer consensus mechanism and ledger node grouping. The multi-layer consensus mechanism enables the sequential completion of the contract computation and the documentation of the computation results on ledgers. The grouping of ledger nodes distributes the workload and facilitates the documentation of different smart contracts on different ledger nodes.

At present, there are pros and cons for all four types of cross-chain technology. Different business scenarios and the technical capabilities of respective projects must be taken into consideration when conducting a holistic evaluation of the said types of cross-chain technology. Evaluation parameters include but not limited to interoperability, trust models, the presence of cross-chain exchanges, the applicability of cross-chain oracles, the support of cross-chain asset mortgage, difficulties in operations and multi-token smart contracts.

2.4.2 ZV CHAIN Cross-chain Protocol

Blockchains are designed to be immutable and traceable. We believe that the burgeoning of DAPP is most likely to be first developed in the field of digital assets, with applications on areas such as supply chain finance, digital copyrights, electronic invoice and gaming. ZV CHAIN supports the mapping and tokenisation of real-life assets, while transactions between users can be executed via the registered assets on the ZV CHAIN network to effect value transfer. Through the tokenisation of assets, even some offline commercial transactions can be locked and managed through smart contracts.

Besides issues such as limited storage space and performance constraints, there is another compelling reason why blockchain projects are yet to be adapted on a large scale to commercial applications, that is individual blockchain project is an isolated Internet of value. It is impossible to settle all commercial projects on one blockchain network. In this respect, multi-chain and multi-ecosystem are not only probable, but also the conceivable future. The challenges of collaborations among various



blockchain projects have considerably impeded the progress of blockchain application development. In response to the problem, ZV CHAIN proposes a cross-chain protocol that supports the value exchange and transfer across various chains.

The ZV CHAIN network is not only an independent blockchain network, but it also materializes cross-chain communications including asset transaction and value transfer. The ZV CHAIN protocol will include the following roles:

- **Interception node**

An interception node functions as full nodes of the original chain by generating new blocks on the original chain and executing transactions. It collects valid transaction information that facilitates cross-chain communications and transmits it to the validation nodes

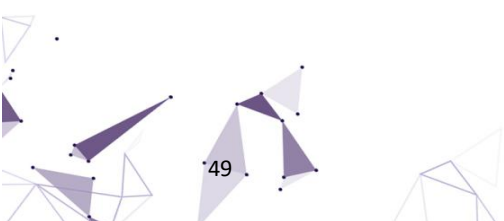
- **Validation node**

A validation node is the notary node of the original chain and the miner node of the ZV CHAIN network that validates the authenticity of the data on the original chain and imbeds it in the new blocks on ZV CHAIN.

- **Gateway node**

A gateway node functions as the wallet node for both the original network and ZV CHAIN, which is equivalent of the gateway between them. It documents and processes transactions in and out of the original chain. This type of nodes requires the allocation of corresponding tokens on the original chain to achieve cross-chain oracle.

ZV CHAIN positions itself as the transit point of the future blockchain world, by integrating user-friendly smart contracts with new business scenarios, and bringing disruptive innovations to traditional business, while enabling all business to implement blockchain technology and laying groundwork for trust and value exchange in the future.





CHAPTER THREE

ZV CHAIN Performance Optimization Proposal

3.1 Sharding and Parallel Computing Framework

The Chiron consensus is able to attain the performance of POS without compromising the features of decentralization and security, and 3000+TPS is powerful enough to support the majority of commercial applications. In consideration of the scalability of ultra-large-scale applications, ZV CHAIN draws inspiration from the MapReduce of Google and the Batch Compute of Alibaba Cloud, and designs a sharding framework that allows the execution of parallel transaction to further improve throughput.

In the parallel computing framework, the heavy nodes are split into computational nodes and proposal node. In other words, in a block generation cycle, multiple proposal nodes are selected based on the random number generated during the previous cycle (For detailed explanations, please refer to the chapter on the Chiron consensus mechanism). On the other hand, nodes selected based on computations from signatures and transaction proposer's addresses are called the computational nodes. The computational nodes are responsible for transaction execution, while proposal nodes manage block generation. The detail workflow of sharing computation is show in Figure. 3.1.

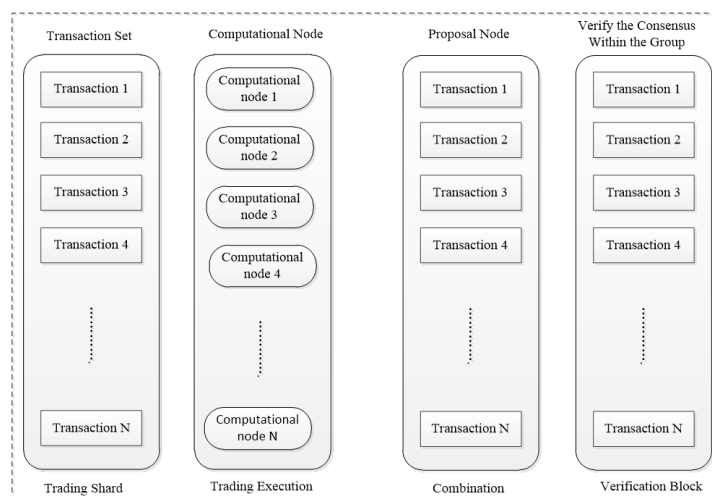
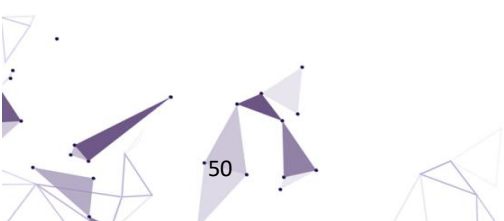


Figure 3.1: Shard Calculation Flowchart





- Transaction shards

The transaction data is sent to different computational nodes based on signatures of the previous block and the proposer's address. There are no restrictions imposed on the receiver's address, rendering our model more flexible than the state channel. Multiple transactions from the same proposer will be transmitted to a single computational node, which in turn can detect double-spending risks within the shortest window period. In the meantime, the VRF algorithm in the Chiron consensus randomly assigns computational nodes as a strategy to distribute transactions to nodes. The multiplexing and the random nature of computational nodes enhance the robustness and security of the system.

- Transaction execution

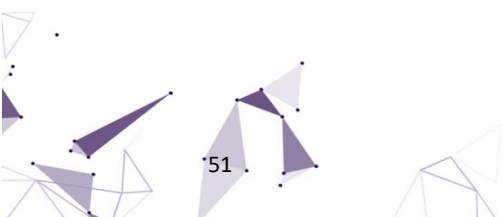
The computational node will carry out transactions according to the, while keeping track of changes in the user accounts. The execution of transactions usually depends on the data of account status, such as account balance and user data stored in the contract. In ZV CHAIN, the complete set of data is stored on computational nodes by design. Whenever a new block is generated, the local status will be updated, therefore, computational nodes can execute transactions locally without performing complex cross-chain interactions.

- Merger

The result of every transaction execution will be submitted to proposal nodes, of which the content includes the Merkle root (hereafter referred to as the root) of account status, the accounts affected by the transaction and the deviation in account status. The proposal nodes will iterate over the results collected and compare local root with the root submitted, to filter the transaction results and consolidate them in to a candidate set. The proposal nodes will then merge the deviations of account status in the candidate set with local accounts to generate the final account status.

- Validation blocks

The validation blocks authenticate the results of transaction execution within the validation groups to generate a group signature and proceed with the final block generation. For detailed illustration, please refer to the part on validation group consensus and block generation under the section of Chiron consensus.



3.2 ZLight Lightning Network

The introduction of Lightning Network technology not only improves the throughput of the system, but also constitutes an integral part of the ZV CHAIN branch structure. The lightning network allows funding transactions to be committed offline securely, with minimal synchronization with the mainchain, instead of frequently updating micropayment in real time on the blockchain network. The with the help of the Lightning Network technology, B2C lightweight connection can be rapidly established to facilitate secure transactions. In addition, ZV CHAIN designs both unidirectional and bidirectional lightning networks that cater to different business scenarios.

3.2.1 ZLight Unidirectional Lightning Network

The unidirectional lightning network is highly accessible. Business owners do not need to put it advance deposit to complete high-frequency low-volume transactions with clients. The unidirectional network is applicable to fast-moving consumer goods business such as sundry shops, mini-mart and small diners. In Figure.3.2, the workflow of the unidirectional lightning network is delineated.

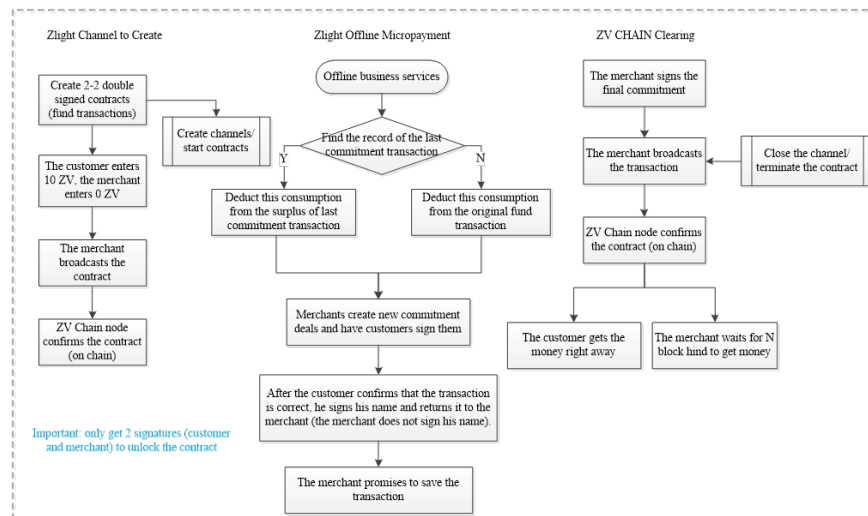


Fig.3.2 The Flowchart of ZV CHAIN Unidirectional Lightning Network

3.2.2 ZLight Bidirectional Lightning Network

The bidirectional lightning network is catered to business owners with relatively high liquidity, such as the supply chain finance, and upstream and downstream. The B2B payment channel supports bidirectional offline asset circulation without compromising the security. The bidirectional lightning network is the standard lightning network channel that supports full-duplex data transmission. The security of the bidirectional lightning network, which allows the transaction to proceed without having to announce it in public, is safeguarded by penalizing the uncooperative participants. The key lies in how to detect and penalize someone when he broadcasts a favorable intermediary commitment transaction on the network. The schematics diagram of how Revocable Sequence Maturity Contract (RSMC) safeguards the system security is illustrated in Figure. 3.3.

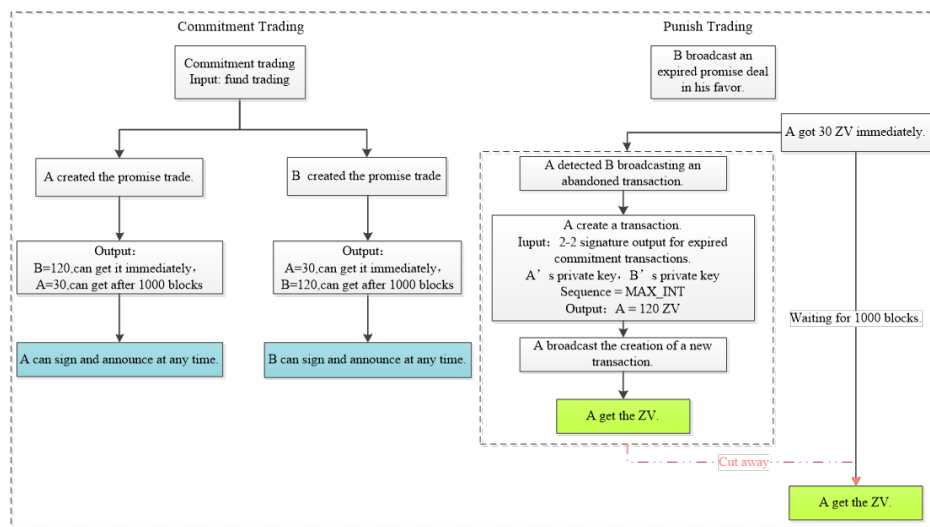


Figure 3.3: ZV CHAIN Bidirectional Lightning Network Security Structure

The ZLight model designs a delayed payment period that regularly sends out transaction notices to a party if its counterpart broadcasts the intermediary commitment transaction on the mainchain and punishes the other party by forfeiting the full transaction amount.

3.2.3 ZLight Branch Structure

The RSMC of the Lightning Network can enhance the throughput of the mainchain. If we were to set up offline payment channels among 1 million customers and 100 thousands business owners, we will need to build $1 \text{ million} \times 100 \text{ thousand} = 10 \text{ million fund contracts}$. Should there be more users or business owners joining the ZV CHAIN mainchain, the number will be magnified in terms of

Cartesian Product. Acknowledging the disparity in scalability of various industries in different regions, ZV CHAIN introduces HTLC to formulate a branch structure. In traditional HTLC, once a node on the chain goes offline or becomes temporarily unavailable, the transaction will be immediately locked, and the asset will remain frozen for a prolonged period, which makes it difficult to maintain a stable and efficient transaction network. ZV CHAIN blazes new trails by innovatively restricting the HTLC depth to two layers and integrating the branch structure. This means that only HTLC nodes authenticated by ZV CHAIN will become the branch nodes of the mainchain. This innovation guarantees the stability of the HTLC services, while capitalizes the returns on each node. The structural design is elaborated in Figure.3.4

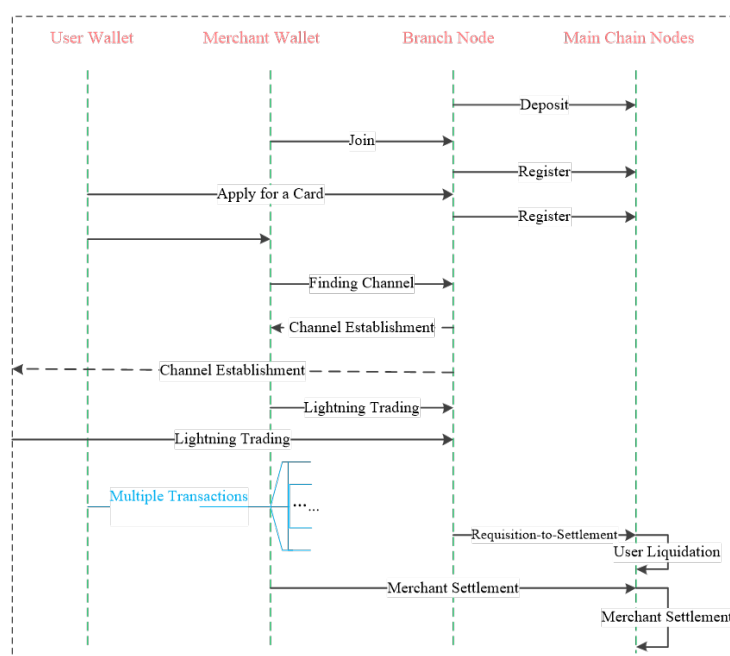


Figure 3.4: ZLight Branch structure

3.3 Distributed Data Storage

The distributed data store encompasses not only block data, but also account balance, contract codes and contract internal data. Let us set an expiry time T_1 for data D , which means that D will be stored on all proposal nodes before T_1 . We refer to data D as hot data, as shown in Figure 3.5.

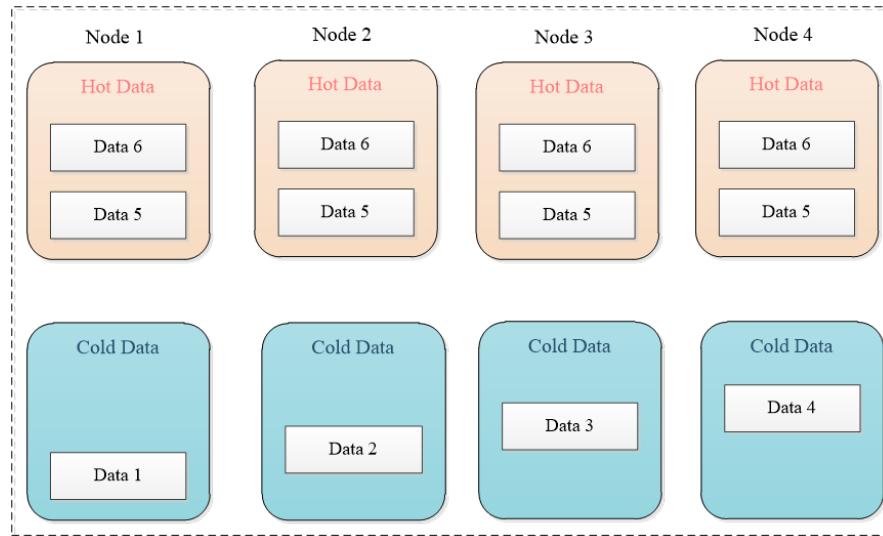


Figure 3.5: Distributed Data Storage and Management—the Diagram of Hot/Cold Data Storage

After T_1 , we will perform a modulo operation on the node ID according to the data hash value, to ascertain the shard in which D is located. (If the node ID is base-16, we can take the first 16 hexadecimal digits and configure 16 groups encoded from 0 to F). Data D will be preserved on the proposal nodes located on the same shard as D, while other proposal nodes will retain the hash of D instead of the original data. The hash of D stored on other nodes is called warm data.

Similarly, let us set an expiry time T_2 for the warm data. After T_2 , the storage of warm data is switched over to storage nodes that are slower and consequently less expensive. The data switched over is called cold data. When historical data is required for transactions during block generation, the network will first read the local data, before searching through the warm and cold data storage nodes. Once found, the data will be validated based on local hash. Once data validation is completed, the storage node that provides the data will be rewarded, otherwise if the validation fails or is timeout, the transaction will not be processed in the block.

3.4 P2P Network

From the perspective of business applications, transaction throughput and latency are the most important trading performance indicators for companies. Key factors affecting the performance of blockchain networks include broadcast communications, information encryption and decryption, consensus mechanism, transaction verification mechanism among several other aspects. As the P2P

network constitutes the core technology of blockchain, the efficiency of P2P communications has a huge impact on the overall performance of the blockchain network. The implementation of light node validation and inter/intra-group communications in the Chiron consensus mechanism both rely heavily on high-performance P2P network. The P2P network of ZV CHAIN performs a significant technical upgrade from the classical model, which is illustrated in Figure. 3.6.

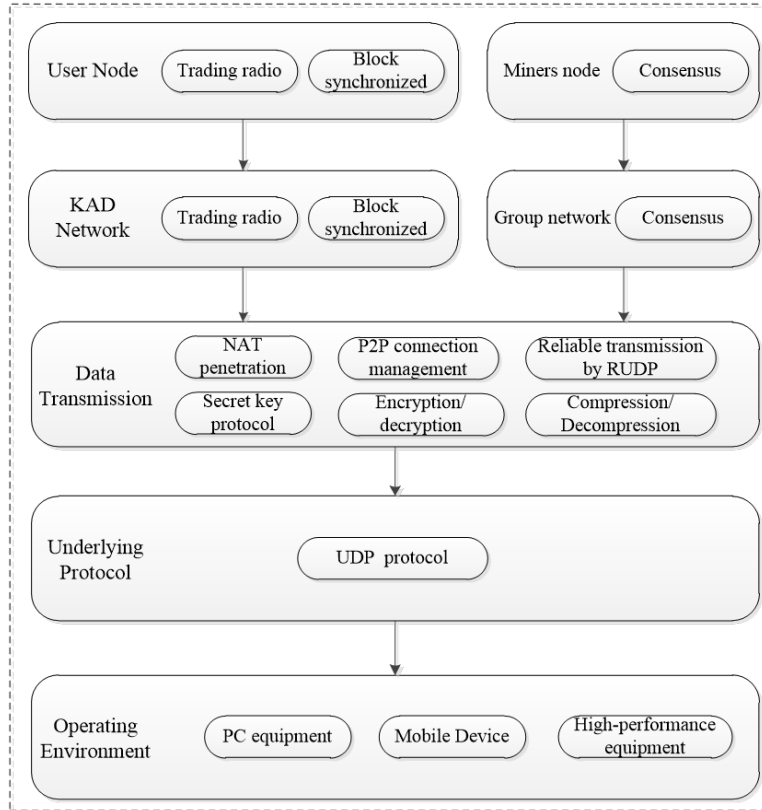


Figure 3.6 ZV CHAIN P2P Architecture

Major improvements include:

- Significantly increased node uptime with the new NAT penetration technology (patent pending);

Table 3.1: Comparison of Intranet Penetration Technology

Internal Network Penetration	STUN	ZV CHAIN P2P
Principle	RFC3489	Linux kernel network protocol stack

Penetration rate	30%	96%
Device Categorization	Full cone / Restricted Cone / Port-restricted Cone / Symmetric Port	Host port / Fixed Port / Symmetric Port
Firewall Penetration	Does not support	Support

- Designed a two-layer KAD network to improve communication efficiency for Chiron's block-by-group approach;
- Using RUDP instead of TCP, reducing the communication latency by approximately 35%.

3.4.1 NAT Penetration

The standard STUN [\[13\]](#) is presented as a solution to the problem facing the mainstream NAT penetration. STUN classifies NAT devices into four categories: full cone NAT, restricted cone NAT, port-restricted cone NAT, and symmetric NAT. We have consolidated statistics from 60,000 Internet cafes in China on the categories of their NAT devices, among which 5% of the Internet cafes use full cone, 7% restricted cone, 58% port-restricted cone and 30% symmetric. A theoretical penetration rate of 56% can be calculated from the following equation :

$$5\% \times 100\% + 7\% \times 100\% + 58\% \times 70\% + 30\% \times 12\% = 56.20\%$$

On the other hand, due to the existence of the NAT firewall, the User Datagram Protocol (UDP) packet in a passive mode, upon reaching the NAT device, will trigger the generation of a corresponding record on the tracking block connected to the port. This side effect will cause a failure of prediction in the subsequent ports and in turn result in the failure of the entire penetration process. STUN does not take into account of the NAT firewall; hence the actual penetration rate is curbed at around 30% -40%.

After a thorough analysis of the Linux kernel protocol stack, we redefine the categorization of NAT devices based on port-forwarding rules, and proceed to re-classify them into three categories, namely host port, fixed port, and symmetric port. By this definition, the statistics collected from 60000 Internet cafes is re-consolidated, among which the percentage of host port is 75%, fixed port 23% and symmetric port 2%. The theoretical penetration rate is thus enhanced to 96% based on the following calculation.



$$75\% \times 98\% + 23\% \times 98\% + 2\% \times 0\% = 96.04\%$$

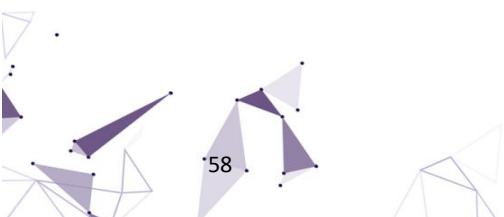
ZV CHAIN solves the problem of penetration failure caused by the change in mapping ports induced by the router/firewall upon receiving non-correlated passive packets, by designing the time-to-live (TTL) dynamic adjustment algorithm. The algorithm enables the actual penetration rate to approach theoretical values.

3.4.2 Multicast Network

All nodes on ZV CHAIN will be added to the global KAD network, where every node will be connected to 8-16 neighbor nodes. The communication between neighbor nodes facilitates the transaction broadcast, block-chain synchronization and group-chain synchronization. ZV CHAIN constructs a two-layer KAD network to locate member nodes and ensures highly efficient communication among group members that in turn expedites the process of proposal submission and validation. The two-layer multicast network has an edge over the global KAD network in terms of accelerating intra-group information transmission and mitigating the load on the entire network.

Table 3.2: Comparison of Communication Protocols

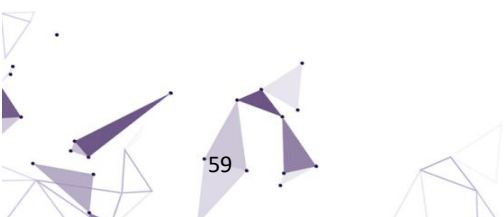
Underlying Protocol	TCP	RUDP
Intranet Node Penetration	Difficult	Easy
High quality network transmission speed	High	High
Moderate quality network transmission speed	Moderate	High (ARQ rapid retransmission)
Low quality network transmission speed	Low	High (FEC redundant transmission)





3.4.3 RUDP

RUDP has significant advantages over TCP in the scenarios of high uptime networks and large amounts of fragmented validation data interaction. From a macro perspective, the industry is gradually moving away from TCP and towards the adoption of RUDP. The QUIC framework proposed by Google, for instance, can be seen as a superset of RUDP. As ZV CHAIN requires high connectivity and collaborative block generation, it has replaced TCP with open-source and mature RUDP in the communication layer.





CHAPTER FOUR

The Technical Architecture of ZV CHAIN

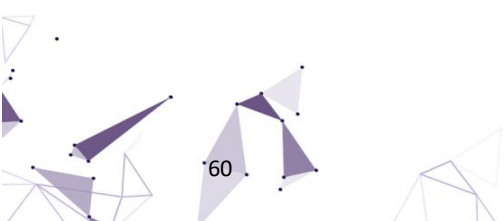
4.1 ZV CHAIN Core Technology Architecture

ZV CHAIN is a native public blockchain which guarantees the decentralization of on-chain application and the immutability of on-chain data. The core businesses running on ZV CHAIN are smart-contract-based decentralized applications. Technologies besides blockchain are adopted to support the smooth running of these Dapps, particularly in the field of finance. On the one hand, the introduction of new technology aims to protect user privacy and trade secrets. For instance, risk control services would benefit greatly from big data and cloud technology, while clearing requires distributed computing clusters; on the other hand, with the help of new technology, we hope to provide a better user experience by integrating existing technologies such as distributed service clusters and CDN to get a better gauge of user expectations and pain points. The framework of the core technology of ZV CHAIN is elaborated in Figure 4.1 below.

4.2 ZV CHAIN Node Architecture

4.2.1 Node Categorization

The ZV CHAIN node is the umbrella term used to describe all participants of the ZV CHAIN ecosystems. We can classify them into four groups according to the ecological roles they play, namely the cornerstone node, the user node, the miner node and the guardian node. The node functions include proposal, validation, storage, risk control and inspection. These nodes can also be classified in three groups based on the minimum requirements for node devices, namely light node, heavy node and supernode. As ZV CHAIN advances into the maturity stage, with the expansion of ledgers on the mainchain network, the mainchain will kick-off the provision of the distributed ledger storage function, the heavy nodes will be subdivided into storage nodes and hashing nodes (also known as computational nodes).



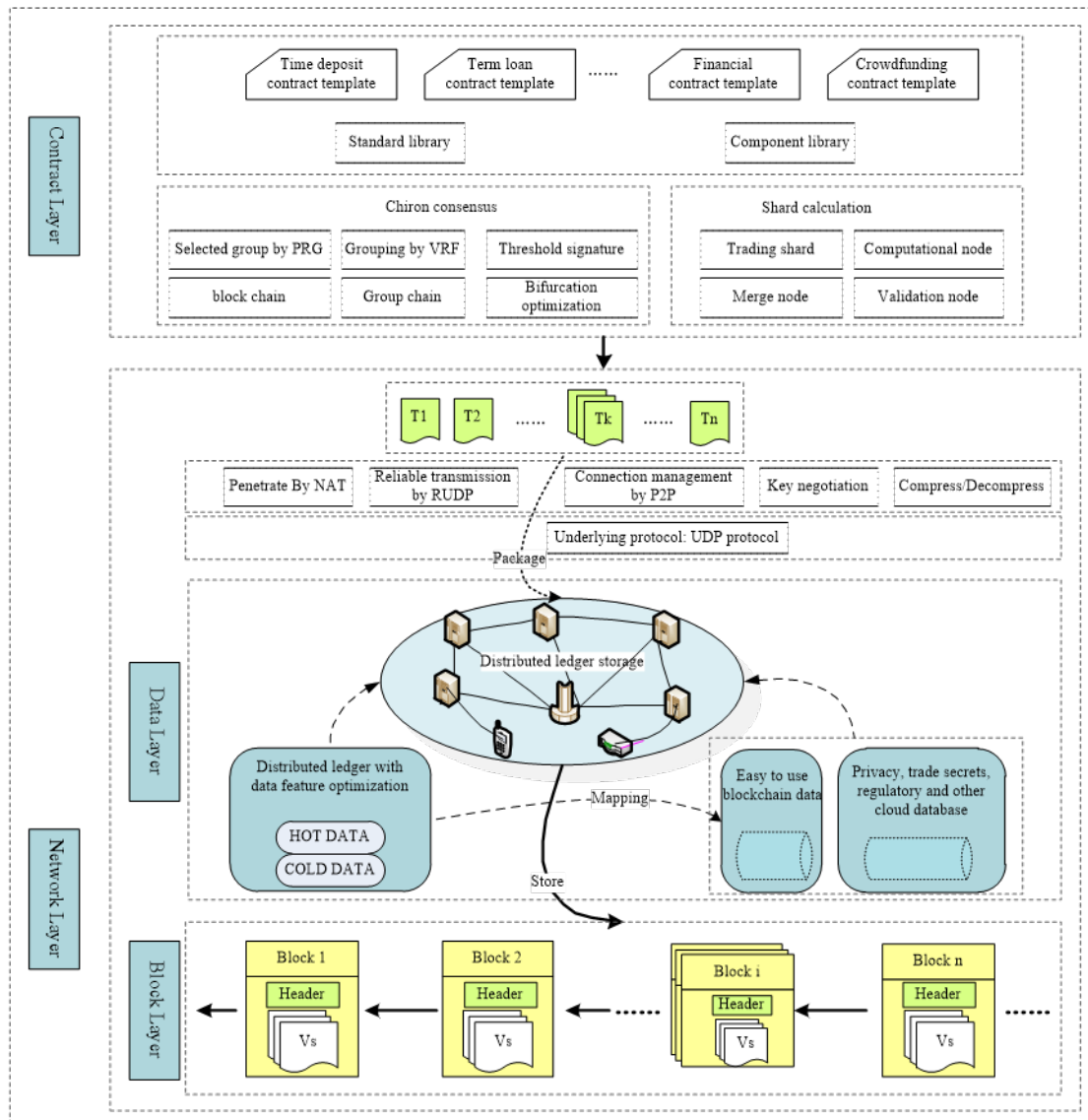


Figure 4.1: ZV CHAIN Core Technology Framework

- User Node (Light Node)

The user node brings liquidity, by virtue of the extensive use of mobile wallet on the ZV CHAIN network, to digital assets in the ecosystem. User nodes can receive incentives by participating in the submissions of proposals. The longer they remain active online, the more incentives they will get.

Table 4.1: ZV CHAIN Node Job Divisions and Functions

Role Dimensions	Device Dimensions	Validation	Proposal	Storage	Risk Control	Inspection
Foundation Node	Cornerstone Node	✓ (Initial Stage)	✓ (Initial Stage)	✓	✓	✓
User Node	Light Node	✓				
Miner Node	Hashing Node	✓	✓			
	Storage Node	✓		✓		
Guardian Node	Supernode			✓	✓	

- Miner nodes (Hashing nodes and storage nodes)

The miner node provides the underlying infrastructural support, with the aid of low-consumption network devices, such as home NAS or AP, to the ZV CHAIN ecosystem. Incentives are gained by participating in the validation process of block generation and ledger storage.

- Guardian node (Supernode)

The guardian node, the network sentinel authorized by the user and miner communities collectively, provides security and risk management services for all users in the ZV CHAIN ecosystem, in addition to offering regulatory services. Both services are made possible by a high-



performance distributed cluster. The guardian nodes in the ZV CHAIN ecosystem receive incentives from real-time risk calculations and full ledger storage.

- Foundation node (Cornerstone node)

The cornerstone node, which is the smallest configuration in the ZV CHAIN, is a node commissioned by the ZV CHAIN Foundation. At the system's initial stage or when it is not yet crowded with external miners, the cornerstone node will assume the function of the proposal node, the validation node, the storage node, and the supernode to ensure the operation of the system. As the number of external miners increases, or after the number of proposal nodes or validation nodes exceeds the threshold value, the cornerstone node no longer performs the said functions; but rather focus on the role of monitor and inspection wither parts of the storage and risk control functions preserved. When the external miner nodes are dwindling, the cornerstone node can be converted to undertake the tasks of proposal submission, validation and more.

4.2.2 Node Function

The node architecture of ZV CHAIN is shown below in Figure 4.2, which includes five major types of nodes:

1. Proposal node

The proposal node is responsible for proposing blocks for the candidate sets

2. Validation node

The validation node has the responsibility of validating candidate block

3. Storage node

The storage node oversees storing distributed data in the system

4. Supernode

The supernode is responsible for storing the risk management data and providing customers with risk control services. The supernode on the ZV CHAIN network aims to help perform the day-to-day function of the ZV CHAIN banking services, while providing nodes that offer complementary services apart from Bitcoin nodes. These complementary services include smart risk control and clearing services provided by weak decentralized nodes.

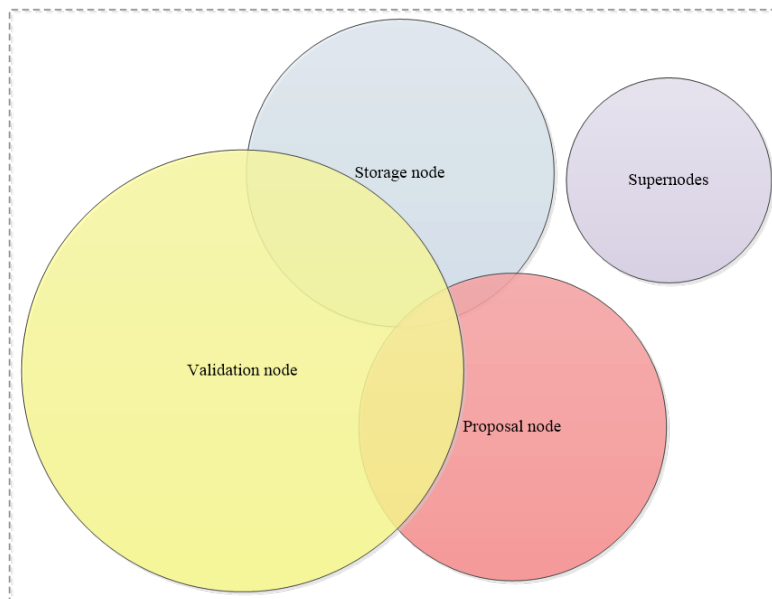


Figure 4.2: Schematic diagram of the ZV CHAIN node function

5. Cornerstone node

The cornerstone node, the smallest configuration of the system, is independently developed by the project team.

During the initial stage or the network is not crowded with external miners, the cornerstone node will assume the function of proposal nodes, validation nodes, storage nodes, and supernodes to ensure the smooth running of the system. As the number of external miners increases, or after proposal nodes or validation nodes exceed the threshold, the cornerstone node no longer performs the functions of proposal submission or validation; rather, it enacts the role of monitor and inspection, while partially retaining storage nodes and supernodes). When the number of external miner nodes is lacking, the cornerstone node can be converted to undertake the tasks of proposal and verification to ensure the smooth sailing of the system.

4.2.3 Node Relations

The function of the user node on the ZV CHAIN network is two-fold: it is the actual user of the system while actively contributing to the liquidity of the network. The user nodes have to pay the miner nodes a levy in order to gain access to the network. In the meantime, the user nodes are entitled to the miner revenue in accordance with their contribution to the liquidity of the system. In addition, the user

nodes are empowered to regularly nominate guardian nodes through voting. The economic and ecological relations among nodes are depicted in Figure.4.3

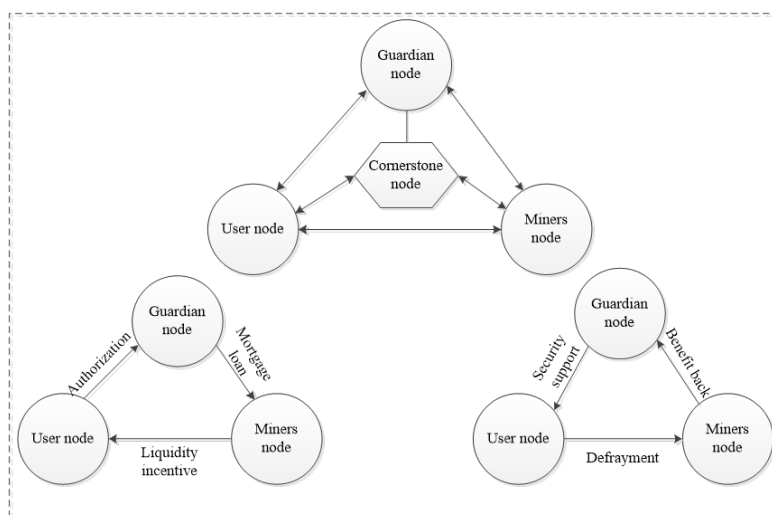


Figure 4.3: Economic Ecological Relations of ZV CHAIN Node

The miner nodes constitute the infrastructure of the ZV CHAIN network. In order to prevent potential fraud and malpractice that may be detrimental to the establishment of the ZV CHAIN network, it is imperative to assess the credibility of miners and their contribution to the network for all mining activities in the Chiron consensus. The indicators of credibility and contribution largely depend on the number of ZV tokens staked and the duration of continued online activities. If the number of ZV tokens staked is less than the requirement, the miner nodes can loan from the guardian nodes to gain the maximum incentives. The guardian nodes safeguard the security of the ZV CHAIN network. The number of user nodes determines the number the guardian nodes, which provides secured risk control services to the user nodes, and loan and mortgage services to the miner nodes.



CHAPTER FIVE

Technical Roadmap and Milestones

1. **Phase I** (Sept 2018 – Aug 2019) - **Mainnet Launch**

Using highly forward-looking Chiron Consensus Mechanism, we will focus on performance optimization and stabilization testing of ZV CHAIN, as well as ledger system suitable for potential applications in financial services. ZV Wallet will come live online as the native digital asset wallet compatible with ZV Chain. We will collaborate with ecosystem partners in financial services, cross-chain and privacy computing. In the last stage of Phase 1, ZV CHAIN will complete its mainnet launch.

2. **Phase II** (Sept 2019 – Feb 2020) - **Ecosystem Cross-chain**

We will prepare beta-stage ZV SDK for developers. ZV CHAIN will complete connection with Cosmos Hub in Phase 2 to link up with BTC and ETH ecosystem. ZV wallet will also complete connection with ZV CHAIN and become LAPP via Lightning Network.

3. **Phase III** (Mar 2020 – Aug 2020) - **Distributed Storage**

ZV CHAIN will undergo further upgrade. The official version of ZV SDK and various financial service middleware will come live. ZV Wallet will also undergo continuous upgrading both to improve user security and to connect the protocol with more business scenarios. As the ecosystem is coming into shape, the increment of full ledger and financial privacy data will drive us to keep perfecting the solutions for distributed storage.

4. **Phase IV** (After Sept 2020) - **Privacy Computing and Smart Finance**

We will find a real blockchain solution for privacy computing. As the ecosystem of data value flow becomes mature. We will incorporate smart finance modules to upgrade the ecosystem into a comprehensive smart self-governing community. The entire ZV ecosystem will also enter a new realm.

ZV CHAIN References

- [1] S. Micali, M. Rabin and S. Vadhan. Verifiable Random Functions. 40th Foundations of Computer Science (FOCS), New York, Oct 1999.
- [2] Wang C, Wang Q, Ren K, et al. Privacy-preserving public auditing for data storage security in cloud computing[C]//2010 proceedings ieee infocom. Ieee, 2010: 1-9.
- [3] Sharding FAQs In URL <https://github.com/ethereum/wiki/wiki/Sharding-FAQs>.
- [4] Jeffrey Dean and Sanjay Ghemawat. MapReduce: Simplified Data Processing on Large Clusters. OSDI 2004.
- [5] Zhao J L, Fan S, Yan J. Overview of business innovations and research opportunities in blockchain and introduction to the special issue[J]. 2016.
- [6] Kastelein, R.” IBM Fuses Blockchain, AI and Cloud Computing into One Unit.”
- [7] Dhillon, Vikram, David Metcalf, and Max Hooper. “Recent Developments in Blockchain.” Blockchain Enabled Applications. Apress, Berkeley, CA, 2017. 151-181.
- [8] DFINITY White Paper: Consensus System. In URL <https://dfinity.org/pdf-viewer/pdfs/viewer?file=../library/dfinity-consensus.pdf>. 2017.
- [9] McEliece R J, Sarwate D V. On sharing secrets and Reed-Solomon codes[J]. Communications of the ACM, 1981, 24(9): 583-584.
- [10] 2018 Deloitte Millennial Survey Millennials Disappointed in Business, Unprepared for Industry 4.0. 2018.
- [11] Buterin V. Chain interoperability[J]. 2016.
- [12] Underwood, Sarah. “Blockchain beyond bitcoin.” Communications of the ACM 59.11 (2016): 15-17.
- [13] Iansiti, Marco, and Karim R. Lakhani. “The truth about blockchain.” Harvard Business Review 95.1 (2017): 118-127.
- [14] Batsaikhan U. Cryptoeconomics—the opportunities and challenges of blockchain[R]. 2017. 60
- [15] Atwood, Mark. “Blockchain Technology Explained:(2018).” (2018).
- [16] Pittenger, David J. “The utility of the Myers-Briggs type indicator.” Review of Educational Research 63.4 (1993): 467-488.
- [17] Samaniego, Mayra, and Ralph Deters. “Blockchain as a Service for IoT.” Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), 2016

IEEE International Conference on. IEEE, 2016.

- [18] Middleton, Stuart E., Nigel R. Shadbolt, and David C. De Roure. "Ontological user profiling in recommender systems." *ACM Transactions on Information Systems (TOIS)* 22.1 (2004): 54-88.
- [19] NIST, "Sha-3 standard: Permutation-based hash and extendable-output functions,"2015.
- [20] B. David, P. Gaži, A. Kiayias, A. Russell, Ouroboros Praos: An adaptively-secure, semisynchronous proof-of-stake blockchain. *EUROCRYPT* 2018.
- [21] F. Vercauteren, Optimal pairings, *IEEE Transactions on Information Theory*, vol. 56, no. 1, pp. 455–461, 2010.



Appendix A: Technical Glossary

A.1 Chiron Consensus Terms and Symbols

p: large prime numbers, cryptographic parameters, such as 256-bit prime number.

GF(p): A finite prime field based on p.

Node: We refer to the client portal running on a user device as a node. According to the hash power of the device, the node can be classified into two types based on the property and configuration: light node and heavy node.

Heavy node: computing PC, professional equipment (mining machine), etc.

Light node: ordinary PC, mobile phone, set-top box, mobile device, embedded device, etc.

Miners: Ordinary users can participate in distributed ledger by signing up an account. Let M be the set of all miners, and label them as $1, 2, \dots \in |M|$. The miners are classified as proposer and verifier according to different functions

Proposer: The full ledger node, responsible for raising proposals

Verifier: nodes that work in a collaborative manner and validate the authenticity of the blocks nominated by the proposers and reach a consensus within the group.

Group: At any given time, for some or all $i \in M$, one or more subsets are arranged, $G_1, G_2, \dots \in |M|$. These subsets are called “group”. We will organize the proposers and the verifiers, according to a preset ratio, into a working group. Each working group has the same group size $n = |G_4|$.

Slot: Slot is the time taken to generate a block. The number of slots is correlated to the height of the block: in the r^{th} slot, a block is generated with a height of r . If however, the block generation process fails during the r^{th} slot, then the block with height r does not exist, while the prehash of the $(r + 1)^{\text{th}}$ block points to the $(r - 1)^{\text{th}}$ block.

Epoch: An epoch contains a number of slots, which is determined by the corresponding preset system parameters.

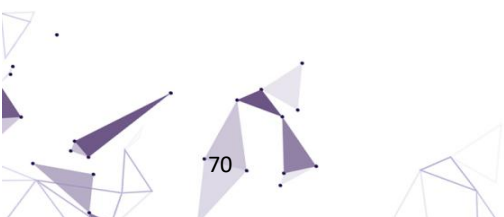
Parent group: After the number of applications to become miners meets the conditions for establishing a group, a new group will be initiated by the working group, which becomes the parent group of the new group. The parent group can assign special attributes to the new group, such as the activation of the new group.

Group survival period: refers to the time between the activation and deactivation of the working group, which is a parameter set by the system. When the time reaches the deactivation stage, the working group will be dismantled.



Miner health index: This index is a multifactorial function. Currently, we consider the following factors (ranked according to priority from high to low):

- Number of participations in block generation (proposals or verifications)
- Participation rate (number of actual participation/the number of theoretical participations)
- The health level of devices (obtained from device fingerprint)
- Number of groups joint (duration of online activities)
- Proof of Stake





A.2 Entities in the Settlement Network

Each of the following entities (network nodes or technical nomenclatures) will be part of the settlement network of ZV CHAIN:

1. Consumer (ZV CHAIN wallet user or card user)
Authorized ZV CHAIN user.
2. Business
An entity that accesses the ZV CHAIN settlement network through a terminal POS or wallet, and accepts ZV CHAIN payment and in turn provides goods or services
3. Proxy node
A network node that acts as a proxy between consumers and businesses during transactions and opens unidirectional lightning networks with the user and the business respectively. It also provides liquidity to currency exchange in cross-border payment scenarios
4. Unidirectional lightning network
A technical (clearing) network that allows consumers and business to make high-frequency, low-volume transfers
5. bidirectional lightning network
A technical (clearing) network that allows high-frequency transactions and exchanges between proxy nodes.
6. Dual-signature contract
A contract that is prepaid by one or both parties. The processing of the transaction requires dual signatures.
7. Commitment Transaction
In a dual-signature contract, one party signs and sends the signed transaction to the other party. This can be considered as completing the transaction clearing; the other party signs the transaction and broadcasts it on the blockchain network to complete the transaction settlement.
8. ZV CHAIN settlement network
The ZV CHAIN settlement network is the distributed ledger of ZV CHAIN. The result after the final confirmation of the transaction (i.e. the settlement result) will be broadcasted to the blockchain.

