Attachment VIII – Architecture Mapping of Hyperchain

Section 1 Summary

Platform summary	
Platform ID	*Hyperchain*
Status/Revision	*V1.8.0*
Type	*Permissioned, Consortium*
Domain	*Provide solutions for financial, medical, energy, trade and other fields.*
Description	*Hyperchain provides technical support to companies, government agencies and industry alliances.*

Section 2 Governance & Compliance Functions

Platform governance	
Governance Type	*Permissioned;*
Chain Network Admin	*ACO (autonomous consortium organization)*
Pledge (cost of malicious action)	*The certificate of malicious node will be revoked.*
Description	*Before this, Hyperchain has strict access mechanisms by member management model. If the Byzantine node is spotted, the members of the group will vote on a proposal to remove it from the organization.*

Platform trust endorsement policy	
Type	*Law/Agreement;*
Tool	*Legal Contract*
Policy	*A peer with Ecert and Rcert is verified as validate peer, all validate peers can participate in the endorsement.*

Section 3 Application

Platform Smart Contract mechanism

Language	*Solidity, Java*
Turing Complete?	*Yes*
Compiler	*Solidity; Java*
Runtime VM	*EVM, JVM, HVM*
DevTools	*GoSDK*、*JavaSDK*
Extra Tool(s)	*Hyperchain Radar (Contract data view);* *MQ (Message push);* *Hypervision (visualized monitoring platform)*
Lifecycle	*Hyperchain's VM supports whole smart contract lifecycle management, including contract deployment, upgrade, freeze, and more.*
Description	*Support JVM*、*EVM and HVM with multiple programming languages compiler.* *SDK provides many interfaces to facilitate application development as a tool for application to interact with hyperchain.*

Section 4 Protocol

Platform AAA Management	
Account type	*Identity; address; …*
Distributed ID	*PKI structure, a digital identity encapsulated in an X.509 digital certificate.*
AAA support	*Hyperchain CA;* *CFCA.*
Description	*Authority control is at the Namespace level, which means that each Namespace will have a corresponding CaManager for CA certificate management and authority control at the Namespace level. The CA system is mainly used for node authority control and transaction authority control.*

Platform Consensus Mechanism	
Algorithm	*RBFT(Robust Byzantine Fault Tolerant) ;*

Consensus mode	*Event;*
Management solution	*Internal*
Description	*RBFT adds active recovery and dynamic node addition and deletion mechanism by optimizing PBFT execution process. Under the premise of ensuring strong consistency of node data, RBFT improves the overall transaction throughput capacity and system stability of the system.*

Platform Ledger Management	
Model	*Account*
Extra	*HMT(HyperMerkle Tree)*
Description	*HyperMerkle trees combine the advantages of both Merkle trees and hash tables, greatly increasing the speed of ledger hash calculations.*

Section 5 Resources

Node Management	
Node Role	*Validate peer (VP);* *Candidate validate peer (CVP);* *Non-validate peer (NVP).*
Joining	*Node will be joined in chain when the entity is allowed to join the consortium, the CAs for node will be offered, then node will be started with CAs.*
Leaving	*Node will be deleted when it become a byzantine node.*
Role changing	*When VP is failover, the CVP node will become validate node.*
Description	*Hyperchain consists of validate peers (VP), candidate validate peers (CVP) and non-validate peers (NVP):* *Validate node refers to the node participating in consensus validate in the blockchain network.* *Candidate validate node refers to node which is the candidate of validate node, when validate node is failover, this node will be become validate node to join consensus.* *Non-validate node refers to the node in the blockchain network that does not participate in consensus validate and only participates in accounting and needs to connect the validate node.*

Platform Data Storage Mechanism	
Mass storage mitigation[1]	*Data Archiving*
Decentralized Data Storage Support	*TiKV*
Data Privacy Solution	*End-to-End TLS encrypted data;* *namespace;* *private transaction.*
Tamper Proof (tamper cost)	*More than 1/3 nodes tampered.*
Description	*Namespace can protect privacy of business layer.* *Private transaction can protect privacy on transaction layer.*

Platform Network Management	
Node Scalability	*Hundreds*
Network Structure	*Distributed; Flexible*
Network Discovery Protocol	*gRPC*
Byzantine Node Accepted?	*Yes*
P2P?	*Yes*
Data Exchange Protocol	*gRPC*
Description	*gRPC uses protocol buffers to connect data centers with pluggable load balancing.*

Section 6 Utils

Platform Messaging Mechanism	
Protocol Type	*gRPC;*
Description	*Further description if any*

[1] On chain storage cost much, solution/mechanism to resolve the problem of large cost of mass storage from node perspective. E.g., data maintenance, data storage and data cleaning.

Platform Crypto Libraries	
Secure Network Connection Type	*TLS; …*
Cipher Suites	*SHA; SM3; ECDSA; SM2; ECDH; AES; SM4; SM9*
Description	*Hyperchain uses SHA and SM3 for hash, supports ECDSA and SM2 for signing. ECDH is used for key agreement, and AES or SM4 for message transmission.*

Section 7 Operation & Maintenance

Platform system management – Node	
Log	*Yes*
Monitoring	*Provides* a *visualized monitoring platform named Hypervision.*
Description	*Hypervision is designed for real-time monitoring and alarms on blockchains, as well as management of smart contracts.* *IPC command can be used to manage network connections, make log-level modification, query license information and so on.*

Platform system management – Chain Network	
Permission Control	*Yes*
Auditing	*Security testing of transactions*
Supervisory Support	*The supervisor can join the blockchain network as a node.*
Description	*Do security testing on extra of the transaction before it's written into the block, failed transactions will become invalid.*

Section 8 External Resource Management

Platform External Resource Management	
Interoperation solution	*Oracle pushes third-party data to Hyperchain, and the smart contract can obtain data information from a specific blockchain address.*
Description	*Oracle provides externally trusted data sources which are authoritative, accurate, non-tamper, stable, and acceptable for auditing, such as databases, trusted timestamps, etc.*

Section 9 Extensions

Platform Extensions - optional	
[the following list can be duplicated for multiple extensions]	
Name	*Smart Contract Support*
Extension type	*Internal*
Extension mode	*Vertical*
Solution	*Hyperchain has accessed multiple virtual machines: EVM, JVM, HVM.*
Serve domain	*Smart Contract Support*
Description	*The smart contract engines support Solidity and Java, they are user-friendly. Contracts are easy to compile and deploy on Hyperchain, all contracts are compatible and portable.*

Platform Extensions - optional	
[the following list can be duplicated for multiple extensions]	
Name	*Inter Blockchain*
Extension type	*External*
Extension mode	*Horizontal*
Solution	*Heterogeneous blockchains with Application chains, side chains and etc.*
Serve domain	*Cross Chain Applications*
Description	*Inter Blockchain supports for inter-chain transactions between homogeneous and heterogeneous blockchain platforms to form blockchain internet.*