Attachment XI – Architecture Mapping of Monero

Section 1 Summary

Platform summary	
Platform ID	*Monero/XMR*
Status/Revision	*Mainnet – v0.14.1.0*
Type	*Public*
Domain	*Peer to peer payments, Financial*
Description	*Monero is an open-source, decentralised, permissionless, fungible cryptocurrency.* https://github.com/monero-project/monero

Section 2 Governance & Compliance Functions

Platform governance	
Governance Type	*Permissionless*
Chain Network Admin	*Community (public)*
Pledge (cost of malicious action)	*Resources (hardware + electricity) – measured by hash rate (H/s)*
Tamper Proof (tamper cost)	>50% of network H/s
Description	*Monero is an open-source project to which everybody is allowed to contribute. There are no restrictions on participation. There is no formal entity (neither for-profit nor foundation) governing the project.* *Improvements to the protocol are discussed on public communication platforms such as GitHub, IRC, Reddit. Regular development meetings, accessible to all, take place on IRC and allow to discuss relevant topics or gauge interest for specific features.* *As one of the defining characteristics of the project since the beginning, Monero is set to undergo regular "protocol upgrades" (also called hard forks) allowing to deploy protocol upgrades.* *https://getmonero.org*

Platform trust endorsement policy	
Type	*Elliptic curve cryptography*
Tool	*Curve Ed25519*
Policy	*CryptoNote protocol, cryptographic signature, one-dimensional distributed acrylic graph (DAG), Schnorr-style multilayered linkable spontenerous anonymous group signatures (MLSAG), Schnorr-style Borromean ring signatures, amounts concealed with Pedersen commitments* *https://getmonero.org/library/Zero-to-Monero-1-0-0.pdf*

Economic Model (optional)	
Price Model to Deploy Contracts and do Transactions	*Minimum fee per kB: fkB =* $f_b^{kB} * (300kB/M100) * (B^{actual}/10)\ b$ Transaction size is round up to the nearest kB.
Who pays the costs of the network	*User*
Monetary Policy of Tokens	*Block rewards uses a formula: [(L-M) >> 19] /* 10^{12} *Steady rate 'tail emissiom' supply of 18.132 million coins by ca. end of May 2022; and 0.3 XMR per minute thereafter.* *Monero is mined with respect to 'coinbase rewards'. Miners receive the coinbase reward along with write permissions for appending the next block to the ledger.*
Rights of Tokens	*N/A*

Section 3 Application

Platform Smart Contract mechanism	
Language	*N/A*
Turing Complete?	*N/A*
Compiler	*N/A*
Runtime VM	*N/A*
DevTools	*N/A*
Extra Tool(s)	*N/A*
Lifecycle	*N/A*

Description	*N/A*

Section 4 Protocol

Platform AAA Management	
Account type	*UTXO*
Distributed ID	*There is no identification system attached to wallet addresses or transactions. The project is entirely permissionless and anyone is free to participate.* *Addresses are based on a dual-key mechanism allowing them to never appear on the blockchain. An address is used by senders of transactions to generate a derived one-time destination. These one-time destinations cannot be related by observers to a particular address or linked together even if they are generated from the same address.*
AAA support	*N/A*
Description	*This dual-key mechanism (also called "stealth addresses") is one of the mechanisms used by Monero to protect users' privacy and ensures token fungibility. More specifically, this mechanism obfuscates senders, recipients and amount of transactions.*

Platform Consensus Mechanism	
Algorithm	*Currently CNv4 (scheduled update to RandomX)*
Consensus mode	*Proof of Work (PoW)*
Management solution	*Internal*
Description	*Monero has committed to aim at Application Specific Integrated Circuit (ASIC) resistance to increase the decentralisation properties of the network. As the ASIC industry tends to be centralized, and there are many more CPUs in the world than ASICs, a CPU friendly PoW algorithm should lower the barrier to entry for miners. As such, the project has developed a new PoW algorithm. In particular, the next protocol upgrade (~October) should include "RandomX", a state-of-the-art algorithm in that domain.* *https://github.com/tevador/RandomX*

Platform Ledger Management	
Model	*Balance*
Extra	*Merkle tree*

Description	*Block structure consists of three parts: block header, base transaction body, and a list of transaction identifiers. The block header has information about the major (protocol version)/minor (miner voting mechanism, albeit currently unused) header version, block creation time, identifier of previous block, and nonce.*

Section 5 Resources

Node Management	
Node Role	*Full Nodes and Pruned Nodes.*
Joining	*Anyone can join the network. A new node simply needs to synchronized with the current state of the chain in order to fully participate.*
Leaving	*Any node can leave at any time.*
Role changing	*N/A*
Description	*N/A*

Platform Data Storage Mechanism	
Mass storage mitigation	*Blockchain pruning - non-critical information removed from local storage. Pruned nodes remove approximately 2/3 of the total blockchain size.*
Decentralized Data Storage Support	*N/A*
Data Privacy Solution	*Ring Signatures, Stealth Addresses, Ring Confidential Transactions (incl. Bulletproofs).*
Description	*A number of privacy-preserving mechanisms are deployed within the Monero protocol. This ensures as little distinguishing information is published to the public ledger as possible whilst maintaining information verifiability, accountability, and audibility.* *This mitigates against PII (personal identifying information) encroachments, breaches of current information and data legislation (GDPR), corporate data harvesting, information surveillance, and mitigates against any destabilization of the fungible nature of the value exchange mechanism.* *These mechanisms are critical to Monero's aim at preserving privacy and constitute a major part of its technical design. The project is constantly pushing the state-of-the art in that domain to ensure these fundamental characteristics.*

Platform Network Management

Node Scalability	*No upper bound. (current ~2000 nodes).*
Network Structure	*Distributed*
Network Discovery Protocol	*Levin Protocol (https://github.com/xmrdsc/py-levin)*
Byzantine Node Accepted?	*Yes*
P2P?	*Yes*
Data Exchange Protocol	*TCP*
Description	*Nodes request and share list of peers from other nodes.*

Section 6 Utils

Platform Messaging Mechanism	
Protocol Type	*RPC*
Description	*JSON-RPC is a stateless, lightweight remote procedure call (RPC) protocol. Primarily this specification defines several data structures and the rules around their processing. It is transport agnostic in that the concepts can be used within the same process, over sockets, over HTTP, or in many various message passing environments. It uses JSON (RFC 4627) as data format.* *https://github.com/monero-project/monero/wiki/Daemon-RPC-documentation* *https://github.com/monero-project/monero/wiki/Wallet-RPC-Documentation*

Platform Crypto Libraries	
Secure Network Connection Type	*P2P; RPC; DNS*
Cipher Suites	*ECDHE-ECDSA-CHACHA20-POLY1305-SHA256; ECDHE-ECDSA-CHACHA20-POLY1305; ECDHE-ECDSA-AES256-GCM-SHA384; ECDHE-ECDSA-AES128-GCM-SHA256; ECDHE-RSA-CHACHA20-POLY1305; ECDHE-RSA-AES256-GCM-SHA384; ECDHE-RSA-AES128-GCM-SHA256*
Description	*Current code uses CHACHA20-POLY1305 by default (with option of above suites)*

Section 7 Operation & Maintenance

Platform system management – Node

Log	*Yes*
Monitoring	*monerod*
Description	*monerod is the daemon client that manages all interactions with the Monero network. It offers necessary features to act as a node. Additionally, it also acts as the interface between wallet software and the Monero network. This allows the wallet software to be completely decoupled from the node management daemon.*

Platform system management – Chain Network	
Permission Control	*N/A*
Auditing	*Auditing mechanisms are self contained within each wallet and pertains to each wallet address managed by the wallet software. There is no network wide auditing system. However, an important auditing mechanism is associated to addresses (or individual transactions). A 'view key' is associated to an address, which gives anyone holding it auditing functionality -- while not allowing any wallet spend authority.* *This functionality would allow, for example, an NGO to publish its view key along with a donation address, so that anyone who wishes can audit received donations. It also allows businesses and individuals to comply with certain regulations, if they are required, to provide visibility over wallet information.*
Supervisory Support	*N/A*
Description	*N/A*

Section 8 External Resource Management

Platform External Resource Management	
Interoperation solution	*N/A*
Description	*N/A*

Section 9 Extensions

Platform Extensions – optional	
[the following list can be duplicated for multiple extensions]	
Name	*N/A*

Extension type[1]	*N/A*
Extension mode[2]	*N/A*
Solution	*N/A*
Serve domain	*N/A*
Description	*N/A*

[1]Standing from DLT system instance perspective, any extension inside the instance is marked as "internal", while any extension outside the instance is marked as "external"

[2]All extension instances are equal (with similar capability and functional features), targeting for the scalability of DLT instance, marked as "horizontal"; extensions with different functional features, targeting to enforce the capability of DLT instance, marked as vertical. Extension type and mode pair(s) is/are used to describe the extension as to the whole DLT system. E.g., sharding (internal – horizontal), lightning – BTC (external – vertical), Corda Contract (internal – vertical).