Appendix – Behavior Interface Model

Table 1 shows the Behavioral Interfaces that originate from the agent-oriented goal model of BlockVoke.

Table 1: Behavioral Interface Model of BlockVoke

Activity	**Trigger**	**Precondition(s)**	**Postcondition(s)**
Manage Certificate	CA wants to manage a CO's Certificate	CA has a public/private key pair and is capable of managing Certificates	CA has managed a CO's Certificate
Communicate Newly Signed Certificate	CA wants to send the CO's signed Certificate	CA has generated CO's Certificate and has an established mode of comunication with them	CA has communicated Newly Signed Certificate
Generate Certificate	CA wants to Generate CO's Certificate	CO's CSR with information relavant to the Certificate, CO's (wallet) public key, personal private key (for signing), personal (wallet) public key	Generated Certificate with CA's Signature and Multisig address
Sign Certificate		CA's Public Key, Multisig address added to Certificate	Certificate signed by CA
Compute Certificate Fingerprint		Certificate Signed by CA	Certificate Fingerprint computed and added by CA
Create Multisignature address	CA wants to create a multisig address to associate with the Certificate	CO's (wallet) public key, CA's (wallet) public key	1-of-2 Multisignature address
Verify CO's Identity	CA wants to verify CO's Identity before Generating Certificate	CO's CSR	CO's Identity has been verified.
Create Certificate Signing Request (CSR)	CO wants their SSL/TLS certificate signed	Unsigned SSL/TLS Certificiate, Bitcoin/Etherium wallet public key	CSR with public key associated with the wallet address added as an extra attribute

Table 1: Behavioral Interface Model of BlockVoke

Activity	**Trigger**	**Precondition(s)**	**Postcondition(s)**
Verify Certificate	End-User Want's to verify a CO's Certificate	Signed Certificate, CA's public key	Certificate has been verified by an End User
Check Certificate Fingerprint		Signed Certificate with computed Fingerprint	Certificate Fingerprint Verified by End-User
Check Certificate Signature		Signed Certificate, Associated CA's Public Key	CA's Signature on Certificate Verified by End-User
Revoke Certificate	CA or CO wants to revoke a certificate that they have signed/own respectively	Crypto wallet with Small credit amount, Signed Certificate, RFC 5280 Code, Optional CA Indentifier	Certificate has been revoked
Create Revocation transactions			Revocation transactions for a Certificate have been created
Create Tx:Revoke transaction		Hash of Tx:Fund transaction for same Multisig address, Signed Certificate, RFC 5280 Code, Optional CA Identifier, Tx:Fund transaction has been created	Tx:Revoke transaction spending the funds sent to Multisig address in Tx:Fund
Add previous output hash of input address (Multisig address)		Hash of Tx:Fund transaction for same Multisig address	Previous output hash of Multisig address added to Tx:Revoke transaction
Add Input address (Multisig address)		Multisignature address associated with a Signed Certificate	Input address added to Tx:Revoke transaction
Add output address		An output address for spending the funds in the multisig address	Output address added to Tx:Revoke transaction
Add OP_RETURN script		Certificate Signature, Date of Issuance, RFC 5280 Revocation code	OP_RETURN script added to Tx:Revoke transaction

Table 1: Behavioral Interface Model of BlockVoke

Activity	**Trigger**	**Precondition(s)**	**Postcondition(s)**
Add Certificate Signature		Certificate Signature	Certificate Signature added to OP_RETURN script of Tx:Revoke transaction
Add Certificate Date of Issuance		Certificate Date of Issuance in days since 2020-02-02	Certificate Date of Issuance added to OP_RETURN script of Tx:Revoke transaction
Create Tx:Fund transaction		Small credit amount for funding Multisig wallet, Input wallet address containing the funding amount, Multisignature address associated with the Signed Certificate	Tx:Fund transaction has been created
Add previous output hash of Input address		Hash of previous transaction with Input address of Tx:Fund transaction as output	Previous output hash of Input address added to Tx:Fund transaction
Prepare Funds		Small Credit amount	Small credit amount prepared and added to Input address of Tx:Fund transaction
Add Input Address		Input Wallet address	Input address added to Tx:Fund transaction
Add output address (Multisig address)		Multisignature address associated with a Signed Certificate	Output address added to Tx:Fund transaction
Send Revocation transactions		Created Tx:Fund and Tx:Revoke transactions	Revocation transactions have been sent to the blockchain network
Add unconfirmed Revocation transactions into mempool	Blockchain network recieves Revocation transactions	Revocation transactions scrutinized by the Blockchain Network	Revocation Transactions added to Unconfirmed transaction List (mempool)
Scrutinize Revocation transactions			Revocation Transactions scrutinized by Blockchain Network

Table 1: Behavioral Interface Model of BlockVoke

Activity	**Trigger**	**Precondition(s)**	**Postcondition(s)**
Propagate mined blocks with confirmed Revocation transactions	Blockchain network recieves a newly mined blocks with confirmed Revocation transactions	Newly mined blocks	Mined blocks with confirmed Revocation transactions propagated on Blockchain Network
Mine Revocation transactions	Miner recieves Revocation transactions from Blockchain Netowork	Unconfirmed Revocation Transactions in Mempool	Revocation transactions mined into a new block and sent to Blockchain Network
Create new block with Revocation transactions		Revocation transactions in Block's transaction list, nonce	Block containing Revocation transactions created
Find nonce		Transaction List containing revocation transactions, Previous block hash	Nonce for block found
Select Revocation transactions from mempool		Revocation transactions in Blockchain Network's mempool	Revocation transactions added to Block's transaction list from Mempool
Mark Certificate as 'Revoked'	User witnesses Tx:Revoke transaction for a Certificate	Confirmed Tx:Revoke transaction	User marks Certificate as Revoked
Communicate Revocation Transactions to Users	Tx:Revoke transaction for a certificate has been confirmed and appears in a block	Certificate fingerprint	User has witnessed a Tx:Revoke transaction on the blockchain with the certificate fingerprint in the OP_RETURN script