

Date	Start Time (24h)	End Time (24h)	Duration (hours)	Week Subtotal	Week Overtime	Notes
Week 53	4/30	5/6				
2022-04-30	0:00	0:30	0.5			(Continued)
2022-05-01	1:00	3:00	2			Backup APIs and verifyByEmail for users
2022-05-01	4:00	7:00	3			Initial review and request for information on Horizon Bridge launch; Research on backup approaches and GCS implementations; Review on Timeless source code pull request related to loading EOTP in memory; Review Timeless proposed security diagram; Provide feedback and guidance on deficiencies and potential areas of improvements
2022-05-01	10:30	11:30	1			(Continued) and research on best GCS approaches for backup services
2022-05-01	19:30	22:30	3			Review of Harmony offsite initiatives; Research, summary, and written plan for Security, Monitoring, Alert initiative
2022-05-02	11:00	13:30	2.5			More granular stats histogram; Repeated runs for stats retrieval and verifications; Fix a bug with blank staking page caused by scientific representation of javascript numbers; Save output for stats histogram; Review suggested fix on tracked tokens (#314)
2022-05-02	17:00	17:30	0.5			Include staked balance for stats histogram; Update key stats numbers
2022-05-04	20:00	20:30	0.5			Sync on recovery address and guardian matters with Timeless
2022-05-06	15:00	17:00	2	15.0		Review strategies, polls, comments, do research and make votes
Week 54	5/7	5/13				
2022-05-07	7:00	9:00	2			Bridge research (watcher mechanisms, trilemma problems, nomad)
2022-05-08	9:00	12:00	3			Bridge research (arbitrum, terra, various major hacks)
2022-05-08	18:00	20:00	2			Review Dionysis presentation, papers, and sync with John on bridge matters
2022-05-10	18:00	19:00	1	8.0		Sync with John on wallet integration matters and bridge development
Week 55	5/14	5/20				
2022-05-18	16:00	17:00	1			Sync with John on bridge development, project structure, and QA
2022-05-20	12:30	13:00	0.5	1.5		Sync with John
Week 56	5/21	5/27				
2022-05-21	12:00	13:00	1			Review and fix various issues reported by SystemDisc (#317 plus some private emails)
2022-05-21	23:30	0:00	0.5			Review and merge #314, #310
2022-05-22	0:00	0:30	0.5			(Continued) and review integration demo issues
2022-05-23	1:00	1:30	0.5			Review bridge PR #31 (canonical cain)
2022-05-23	20:30	21:30	1			Sync with John
2022-05-24	8:00	9:30	1.5			Review bridge PR and code #30, #31 (canonical cain)
2022-05-25	1:00	3:00	2			Review bridge PR and code #31 (canonical cain), #35 (Merkle Patricia Tree implementation), Issue #22
2022-05-25	11:00	15:00	4			Review bridge PR #34 (limiting storage) and #35 (MPT library)
2022-05-25	20:00	23:30	3.5			Review and feedback on bridge PR #37 (developer guide) and #38 (refactor)
2022-05-26	0:00	1:30	1.5			Review bridge PR #38 (refactor); Further feedback and discussion on bridge PR #31 (canonical cain); Further review on #37 (developer guide)
2022-05-27	14:00	15:00	1	17.0		Sync with John
Week 57	5/28	6/3				
2022-06-02	17:00	18:00	1			Bridge development planning and discussions
2022-06-02	20:00	0:00	4	5.0		Bridge research regarding BLS12-381 verification and code review for related golang and smart contract implementations
Week 58	6/4	6/10				
2022-06-06	11:30	12:30	1			Sync with John on challenges of bridge implementation and dividing tasks
2022-06-07	0:00	2:00	2			Research on BLS signature fundamentals
2022-06-07	10:00	11:30	1.5			Turstable bridge contract-based BLS signature verification research and progress update
2022-06-07	15:30	16:00	0.5			Sync with John (ETH Light Client and various issues to debug)
2022-06-07	20:30	21:00	0.5			Continuing to debug
2022-06-07	23:00	0:00	1			Research on BLS signature fundamentals and reviewing original paper
2022-06-08	0:00	2:30	2.5			(Continued) and review bridge #38 (refactor)
2022-06-08	11:30	16:30	5			Research and feedback on light client proxy proposal based on Intel SGX; Discussion and analysis regarding Intel SGX based BLS12-381 verification approaches, smart contract verification complexity, and feasibility of using ZKP verification, as well as available tools; Research on miller loop and ways to simplify; Review on EIP 2537; Review solidity-big-number implementations; Review 0xPARC ZKP circuit code for BLS12-381 verification
2022-06-09	0:00	2:30	2.5			Continued review on bridge #37, #38; Deepdive on Intel ECDSA attestation flow and requirements
2022-06-09	11:30	12:00	0.5			Sync with John and debugging IDE and dev environment issues
2022-06-09	21:00	0:00	3			Intel SGX deepdive, feasibility evaluation on SGX attestation verification on contract; Discussion and analysis on SGX related approaches and mechanisms implemented by Avalanche

2022-06-10	0:00	0:30	0.5		(Continued)
2022-06-10	15:00	18:30	3.5		Further research and detailed analysis on ZKP based BLS12-381 verification using 0xPARC prototype; Review EIP-2537 discussions
2022-06-10	21:30	23:30	2	26.0	Further deepdive and Intel DCAP ECDSA architecture, encryption and validation mechanisms, and implementation
Week 59	6/11	6/17			
2022-06-12	17:00	19:00	2		Research and analysis on vulnerabilities related to SGX-based approaches for light-client proxy and watcher mechanisms
2022-06-12	19:30	21:30	2		Research on various curves and precompiles in existing EVM
2022-06-13	3:30	5:00	1.5		Research and detailed analysis on smart contract based BLS12-381 verification and comparing the approach with alternatives; Research on pairing implementation in golang
2022-06-13	13:30	14:30	1		Research and code analysis on BLS-verification contracts by Semar and Celo / Plumo, and existing implementations on EVM
2022-06-13	14:30	15:00	0.5		Sync with John
2022-06-14	2:00	3:00	1		BLS12-381 fundamentals review and signature aggregation and verification methods review
2022-06-14	16:00	16:30	0.5		Sync with John
2022-06-15	15:00	16:00	1		Sync with Semar and Genasha, debugging and discussion regarding smart contract implementation of 384 bit arithmetics and comparison to golang implementations of BLS12-381 verification inside EVM
2022-06-16	10:45	11:45	1		Sync with John and assist Semar on big integer field arithmetic and related libraries
2022-06-16	21:00	23:00	2		Catch up on John's bridge development log and issues in #48 (refactor v2)
2022-06-17	12:30	13:00	0.5	13.0	Sync with John and debugging unchecked arithmetic matters
Week 60	6/18	6/24			
2022-06-20	15:00	15:30	0.5		Smart contract BLS12-381 implementation review and debugging
2022-06-20	20:30	21:00	0.5		script-shim vulnerability alert analysis and conclusion
2022-06-19	20:00	22:00	2		Catch up on John's bridge development log and new issues in #48 (refactor v2)
2022-06-21	10:15	10:45	0.5		Bridge header verification contract code review; Sync with Semar and assist on library deployment without using contract management frameworks
2022-06-21	15:45	16:15	0.5		Sync with John on bridge development update
2022-06-22	15:00	15:30	0.5		Sync with Semar and Genasha, debugging local EVM environment and smart contract BLS12-381 verification implementation
2022-06-24	7:00	10:00	3		Review (trusted) old bridge incident report, analysis, and incident response
2022-06-24	17:00	20:00	3	10.5	Bridge incident analysis and follow up
Week 61	6/25	7/1			
2022-06-25	10:45	11:15	0.5		Sync with John regarding Australian whitehacker lead and bridge hack
2022-06-25	14:00	16:00	2		Bridge incident targeted investigation
2022-06-26	16:00	16:30	0.5		Sync with John regarding bridge hack, trustless bridge development, and next steps
2022-06-27	8:30	9:30	1		Bridge incident transaction flow analysis and investigation
2022-06-27	10:30	18:00	7.5		On-site bridge incident response and investigation, coordination with oversea investigations
2022-06-28	7:30	12:00	4.5		Bridge investigation, sync with FBI, Chainalysis, and others
2022-06-28	12:30	13:00	0.5		Sync with John on bridge development change and NFT initiatives
2022-06-28	13:30	15:00	1.5		Bridge investigation, continued
2022-06-28	22:30	0:00	1.5		Bridge investigation, continued; Suspect profile build-up
2022-06-29	0:00	2:30	2.5		(Continued)
2022-06-29	9:30	11:00	1.5		(Continued) Bridge response briefing; investigation follow up
2022-06-29	11:30	12:00	0.5		Sync with Anchain; Investigation follow-up
2022-06-29	13:00	16:00	3		On-site bridge targeted investigation and suspect profile building
2022-06-29	17:30	18:30	1		Investigation, continued
2022-06-29	21:00	23:00	2	30.0	Investigation, continued
2022-06-30	9:00	11:30	2.5		Suspect profile expansion; Continued investigation
2022-06-30	13:00	18:30	5.5		Investigation, continued; Log analysis
2022-06-30	7:30	10:00	2.5		Continued log analysis; Oversea investigation coordination
2022-07-01	9:00	12:00	3		Investigation follow-up, response to North Korea rumors, sync with Elliptic; Sync with John
2022-07-01	21:00	22:00	1	14.5	Oversea investigation follow-up
Week 62	7/2	7/8			
2022-07-03	20:30	21:30	1		Internal follow up on investigation
2022-07-04	10:30	11:00	0.5		Internal follow up on investigation
2022-07-04	19:00	19:30	0.5		(Continued)
2022-07-05	9:00	10:30	1.5		Chat log review; Suspect profile review; NFT initiative follow ups

2022-07-05	11:30	13:00	1.5		On-site discussions and workshop on several matters: investigation follow-up, SMS Wallet, NFT initiatives, task allocations
2022-07-05	13:00	13:30	0.5		Sync with John on NFT initiative and SMS Wallet tasks
2022-07-05	14:30	18:30	4		On-site discussions of investigation, safety, and NFT minting and wallet requirements; Security and devOps practices review, incident analysis review
2022-07-06	13:30	16:00	2.5		(Continued) and SMS Wallet initial research and mechanism discussions
2022-07-06	17:00	19:00	2		(Continued) and sync on various use cases such as gaming
2022-07-07	14:00	15:00	1		Oversea investigation follow-up and next step preparation
2022-07-08	19:00	22:00	3		SMS Wallet core security mechanisms design
2022-07-08	23:00	0:00	1	19.0	Refining SMS Wallet core security mechanism
Week 63	7/9	7/15			
2022-07-09	0:00	2:00	2		SMS Wallet security mechanism write up and revision
2022-07-10	15:00	16:30	1.5		SMS Wallet security mechanism review and research on phone-number and text-message based wallets
2022-07-11	0:00	3:30	3.5		SMS Wallet full specification (core sections)
2022-07-11	6:00	7:00	1		Q3 initiative and NFT minting platform plan review
2022-07-11	11:45	12:15	0.5		Sync with John on NFT minting initiatives and SMS Wallet
2022-07-11	13:15	18:45	5.5		On-site discussions on gaming, gaming SDK, SMS Wallet, and revising SMS Wallet documentations
2022-07-12	11:45	12:15			
2022-07-12	15:30	18:30	3		On-site discussions and Q&A regarding SMS Wallet and sharable components to Email Wallet and related products; Revision of SMS Wallet documentations
2022-07-13	0:00	1:30	1.5		Revision of SMS Wallet doc and NFT acquisition section
2022-07-13	12:00	16:00	4		On-site discussions regarding gaming, SMS Wallet integrations, NFT minting; Revision of documentations; Bridge hack
2022-07-13	17:00	18:30	1.5		(Continued)
2022-07-13	23:00	0:00	1		SMS Wallet presentation material preparation
2022-07-14	0:00	2:00	2		SMS Wallet presentation deck
2022-07-14	10:30	12:30	2		On-site presentations, SMS Wallet presentation, Q&A, and discussions regarding gaming integrations
2022-07-14	14:00	15:30	1.5		SMS Wallet doc (mini-wallet)
2022-07-14	19:00	20:30	1.5		(continued)
2022-07-15	0:00	2:00	2		SMS Wallet doc (fiat-gateway, offboarding, other notes)
2022-07-15	11:15	12:15	1		Anchain report review and sync up
2022-07-15	12:30	13:00	0.5	35.5	Bridge incident impacted partner follow-up
Week 64	7/16	7/22			
2022-07-16	0:00	2:00	2		Review NFT initiative and gaming SDK presentations and evaluate points of integrations with SMS Wallet
2022-07-16	15:00	17:00	2		SMS Wallet implementation requirement analysis
2022-07-17	14:00	14:30	0.5		Sync with John on NFT initiatives, SDK plans, and roles of SMS Wallet
2022-07-17	15:00	17:30	2.5		SMS Wallet implementation initial setups
2022-07-18	15:30	19:00	3.5		On-site: SMS Wallet implementation using GCP Datastore, Twilio, and server setup
2022-07-18	22:00	0:00	2		Research and implementation on SMS operations, server APIs, and security mechanisms
2022-07-19	0:00	1:00	1		(Continued)
2022-07-19	14:30	18:30	4		On-site: SMS wallet implementation, sync up and planning with Hopsnotch, Q&A on SMS Wallet with various individuals
2022-07-19	22:00	0:00	2		Completing SMS Wallet server side and initial client side package setup
2022-07-20	0:00	2:00	2		(continued) and some client implementations
2022-07-20	13:30	16:00	2.5		On-site: SMS wallet client side implementation, persistence, state management, components; Gaming use cases sync up
2022-07-20	17:00	20:00	3		(continued)
2022-07-20	22:00	0:00	2		(continued) and client side apis
2022-07-21	10:30	11:30	1	30.0	Magic.link research and comparison to SMS Wallet
2022-07-21	13:00	17:00	4		SMS Wallet client side implementation (layout, controls, creation flow); Gaming marketplace partner sync up
2022-07-21	21:30	0:00	2.5		Fix server side bugs for creation flow; Fix saga, reducer, actions; Fix OTP verifications and components; Recovery QR code flow; Utilities, notifications;
2022-07-22	0:00	3:00	3		(Continued)
2022-07-22	10:00	15:30	5.5		Improved notifications, explorer link; Fix issues with web3 APIs, webpack, polyfill, and package dependency bugs; Wallet component; More fundamental components (text, balance, and others); Improve key management
2022-07-22	17:00	0:00	7	22.0	Complete SMS Wallet client implementations (recover, send, logout, and others) and end-to-end flow; Deployment at smswallet.xyz, debugging, and testings

			Regular	210.5		
			Overtime		36.5	
			Total	247.0		