Understand Sui Security

This page provides an overview of the major guarantees Sui provides in terms of security.

Sui asset owners and smart contract designers can start learning here about the mechanisms available to secure their assets, and the assurances Sui provides for them. Smart contract designers can also learn about the overall Sui security architecture to ensure the asset types they design leverage Sui to provide a secure experience to the asset holders.

Sui is designed to provide very high security guarantees to asset owners. Assets on Sui can be used only by their owners, according to the logic pre-defined by smart contracts that can be audited, and that the network will be available to process them correctly despite some of the validators operating Sui not following the protocol correctly (fault tolerance).

The security features of the Sui system ensure a number of properties:

The Sui system is operated by a set of validators that process transactions. They implement the Sui protocol that allows them to reach agreement on valid transactions submitted and processed in the system.

The agreement protocols Sui uses tolerate a fraction of validators not following the Sui protocol correctly, through the use of Byzantine fault tolerant broadcast and consensus. Specifically, each validator has some voting power, assigned to it through the process of users staking / voting for them using their SUI tokens. Sui maintains all its security properties if over 2/3 of the stake is assigned to validators that follow the protocol. However, a number of auditing properties are maintained even if more validators are faulty.

A Sui transaction is valid and can proceed only if the owner of all owned assets it operates on digitally signs it with their private signature key. This signature key can be kept private by the user and not be shared with anyone else. As a result, it is not feasible for any other party to operate on an owned asset of a user undetected, even if all validators do not follow the protocol.

A private signature key also corresponds to a public address on the Sui network that can be used to send a user assets or allow smart contracts to define custom access control logic. A user may have one or more addresses corresponding to multiple signature keys for convenience or privacy reasons. An address does not need any pre-registration, and sending an asset to an address automatically creates this address on the network. However, this means that users should be careful to check the recipient address of transfers, or parties involved in any other operations, as sending assets to an incorrect address may have irrevocable effects.

All assets have a type that is defined within a Sui Smart Contract. Sui provides a few system contracts, such as those used to manage the SUI native token, yet also allows anyone to write and submit custom smart contracts. A transaction on an asset type can call operations defined in only the smart contract that defined the asset type, and is constrained by the logic in the contract.

For this reason, users are encouraged to operate on their assets using smart contracts they trust, that they or others they trust have audited, and understand the logic they define for operations on their assets. Sui smart contracts are defined as immutable assets to allow third parties to audit them and also prevent their modification to increase assurance.

The Move smart contract language is designed with ease of audit and verification in mind. You may be interested in our introduction to Smart Contracts in Move.

Shared assets allow multiple users to operate on them through transactions; that may include some of their owned assets as well as one or more shared assets. These shared assets represent data and logic used to implement protocols that mediate between different users in a safe way, according to the smart contract that defined the type of the shared asset. Sui allows all users to create transactions involving shared assets. But the smart contract type may define additional restrictions on which address and how the shared assets may be used.

A valid transaction submitted to all validators has to be certified and its certificate also has to be submitted to all validators to be finalized. Even if a subset of validators do not follow the protocol, the transaction can be finalized through the remaining validators that correctly follow the Sui protocol. This is achieved through the use of cryptographic Byzantine fault tolerant agreement protocols for broadcast and consensus defined by the Sui protocol. These protocols ensure both safety, meaning that the incorrect validators cannot convince correct clients of incorrect state, and liveness, meaning that incorrect validators cannot prevent transaction processing.

All transactions in Sui have to be associated with a gas asset to cover the cost of processing by Sui. A valid transaction may result in successful execution or an aborted execution. An execution may abort due to a condition within the smart contract defining the asset, or because it has ran out of sufficient gas to pay for the cost of execution. In cases of success, the effects of the operation will be finalized; otherwise, the state of assets in the transaction is not changed. However, the gas asset is always charged some amount of gas, to alleviate denial-of-service attacks on the system as a whole.

A user client can perform the process of submitting the transaction and certificate itself or rely on third party services to submit the transaction and interact with validators. Such third parties need not have user private signature keys and cannot forge transactions on the users' behalf. They can reassure a user client a transaction has been finalized through a set of signatures from validators attesting to the transactions finality and its effects. After that point, the users can be assured that changes the transaction resulted in will persist on the state of Sui.

Sui validators provide facilities for users to read all assets they store, as well as the historical record of transactions they have processed that led to these assets. Validators also provide cryptographic evidence of the full chain of transactions that contributed to an asset state. User clients can request and validate this chain of evidence to ensure all operations were correct and the result of the collective agreement between validators. Services that operate full replicas, mirroring the state of one or more validators, perform such audits routinely.

The public auditability of Sui also implies that all transactions and assets within Sui are publicly visible. Users that are mindful of their privacy may use multiple addresses to benefit from some degree of pseudonymity, or third-party custodial or non-custodial services. Specific smart contracts with additional cryptographic privacy protections can also be provided by third parties.

Sui uses the established Delegated Proof-of Stake model to periodically determine its set of validators. Users can lock and delegate their SUI tokens in each epoch to determine the committee of validators that operate the Sui network in the next epoch. Anyone with over a minimum amount of delegated stake can operate a Sui validator.

Validators operate the network and provide rewards to users that stake their Sui to support them as validators, through gas fee income. Validators with poor reliability, and in turn the users that delegated their stake to them, may receive a lower reward. But user stake cannot be confiscated away either by malicious validators or anyone in the network.

This mechanism ensures that validators are accountable to Sui users and can be rotated out at the first sign of unreliability or misbehavior, including noticed attempts to censor valid transactions. Through choices of validators, and the protocol they are willing to operate, Sui users also have a meaningful say on the future evolution of the Sui system.

If you are looking for an in-depth technical explanation of the computer science behind Sui security, you may have a look at our white paper on the Sui Smart Contracts Platform .

Security features

Sui is designed to provide very high security guarantees to asset owners. Assets on Sui can be used only by their owners, according to the logic pre-defined by smart contracts that can be audited, and that the network will be available to process them correctly despite some of the validators operating Sui not following the protocol correctly (fault tolerance).

The security features of the Sui system ensure a number of properties:

The Sui system is operated by a set of validators that process transactions. They implement the Sui protocol that allows them to reach agreement on valid transactions submitted and processed in the system.

The agreement protocols Sui uses tolerate a fraction of validators not following the Sui protocol correctly, through the use of Byzantine fault tolerant broadcast and consensus. Specifically, each validator has some voting power, assigned to it through the process of users staking / voting for them using their SUI tokens. Sui maintains all its security properties if over 2/3 of the stake is assigned to validators that follow the protocol. However, a number of auditing properties are maintained even if more validators are faulty.

A Sui transaction is valid and can proceed only if the owner of all owned assets it operates on digitally signs it with their private signature key. This signature key can be kept private by the user and not be shared with anyone else. As a result, it is not feasible for any other party to operate on an owned asset of a user undetected, even if all validators do not follow the protocol.

A private signature key also corresponds to a public address on the Sui network that can be used to send a user assets or allow smart contracts to define custom access control logic. A user may have one or more addresses corresponding to multiple signature keys for convenience or privacy reasons. An address does not need any pre-registration, and sending an asset to an address automatically creates this address on the network. However, this means that users should be careful to check the recipient address of transfers, or parties involved in any other operations, as sending assets to an incorrect address may have irrevocable effects.

All assets have a type that is defined within a Sui Smart Contract. Sui provides a few system contracts, such as those used to manage the SUI native token, yet also allows anyone to write and submit custom smart contracts. A transaction on an asset type can call operations defined in only the smart contract that defined the asset type, and is constrained by the logic in the contract.

For this reason, users are encouraged to operate on their assets using smart contracts they trust, that they or others they trust have

audited, and understand the logic they define for operations on their assets. Sui smart contracts are defined as immutable assets to allow third parties to audit them and also prevent their modification to increase assurance.

The Move smart contract language is designed with ease of audit and verification in mind. You may be interested in our introduction to Smart Contracts in Move.

Shared assets allow multiple users to operate on them through transactions; that may include some of their owned assets as well as one or more shared assets. These shared assets represent data and logic used to implement protocols that mediate between different users in a safe way, according to the smart contract that defined the type of the shared asset. Sui allows all users to create transactions involving shared assets. But the smart contract type may define additional restrictions on which address and how the shared assets may be used.

A valid transaction submitted to all validators has to be certified and its certificate also has to be submitted to all validators to be finalized. Even if a subset of validators do not follow the protocol, the transaction can be finalized through the remaining validators that correctly follow the Sui protocol. This is achieved through the use of cryptographic Byzantine fault tolerant agreement protocols for broadcast and consensus defined by the Sui protocol. These protocols ensure both safety, meaning that the incorrect validators cannot convince correct clients of incorrect state, and liveness, meaning that incorrect validators cannot prevent transaction processing.

All transactions in Sui have to be associated with a gas asset to cover the cost of processing by Sui. A valid transaction may result in successful execution or an aborted execution. An execution may abort due to a condition within the smart contract defining the asset, or because it has ran out of sufficient gas to pay for the cost of execution. In cases of success, the effects of the operation will be finalized; otherwise, the state of assets in the transaction is not changed. However, the gas asset is always charged some amount of gas, to alleviate denial-of-service attacks on the system as a whole.

A user client can perform the process of submitting the transaction and certificate itself or rely on third party services to submit the transaction and interact with validators. Such third parties need not have user private signature keys and cannot forge transactions on the users' behalf. They can reassure a user client a transaction has been finalized through a set of signatures from validators attesting to the transactions finality and its effects. After that point, the users can be assured that changes the transaction resulted in will persist on the state of Sui.

Sui validators provide facilities for users to read all assets they store, as well as the historical record of transactions they have processed that led to these assets. Validators also provide cryptographic evidence of the full chain of transactions that contributed to an asset state. User clients can request and validate this chain of evidence to ensure all operations were correct and the result of the collective agreement between validators. Services that operate full replicas, mirroring the state of one or more validators, perform such audits routinely.

The public auditability of Sui also implies that all transactions and assets within Sui are publicly visible. Users that are mindful of their privacy may use multiple addresses to benefit from some degree of pseudonymity, or third-party custodial or non-custodial services. Specific smart contracts with additional cryptographic privacy protections can also be provided by third parties.

Sui uses the established Delegated Proof-of Stake model to periodically determine its set of validators. Users can lock and delegate their SUI tokens in each epoch to determine the committee of validators that operate the Sui network in the next epoch. Anyone with over a minimum amount of delegated stake can operate a Sui validator.

Validators operate the network and provide rewards to users that stake their Sui to support them as validators, through gas fee income. Validators with poor reliability, and in turn the users that delegated their stake to them, may receive a lower reward. But user stake cannot be confiscated away either by malicious validators or anyone in the network.

This mechanism ensures that validators are accountable to Sui users and can be rotated out at the first sign of unreliability or misbehavior, including noticed attempts to censor valid transactions. Through choices of validators, and the protocol they are willing to operate, Sui users also have a meaningful say on the future evolution of the Sui system.

If you are looking for an in-depth technical explanation of the computer science behind Sui security, you may have a look at our white paper on the Sui Smart Contracts Platform .

Security architecture

The Sui system is operated by a set of validators that process transactions. They implement the Sui protocol that allows them to reach agreement on valid transactions submitted and processed in the system.

The agreement protocols Sui uses tolerate a fraction of validators not following the Sui protocol correctly, through the use of Byzantine fault tolerant broadcast and consensus. Specifically, each validator has some voting power, assigned to it through the

process of users staking / voting for them using their SUI tokens. Sui maintains all its security properties if over 2/3 of the stake is assigned to validators that follow the protocol. However, a number of auditing properties are maintained even if more validators are faulty.

A Sui transaction is valid and can proceed only if the owner of all owned assets it operates on digitally signs it with their private signature key. This signature key can be kept private by the user and not be shared with anyone else. As a result, it is not feasible for any other party to operate on an owned asset of a user undetected, even if all validators do not follow the protocol.

A private signature key also corresponds to a public address on the Sui network that can be used to send a user assets or allow smart contracts to define custom access control logic. A user may have one or more addresses corresponding to multiple signature keys for convenience or privacy reasons. An address does not need any pre-registration, and sending an asset to an address automatically creates this address on the network. However, this means that users should be careful to check the recipient address of transfers, or parties involved in any other operations, as sending assets to an incorrect address may have irrevocable effects.

All assets have a type that is defined within a Sui Smart Contract. Sui provides a few system contracts, such as those used to manage the SUI native token, yet also allows anyone to write and submit custom smart contracts. A transaction on an asset type can call operations defined in only the smart contract that defined the asset type, and is constrained by the logic in the contract.

For this reason, users are encouraged to operate on their assets using smart contracts they trust, that they or others they trust have audited, and understand the logic they define for operations on their assets. Sui smart contracts are defined as immutable assets to allow third parties to audit them and also prevent their modification to increase assurance.

The Move smart contract language is designed with ease of audit and verification in mind. You may be interested in our introduction to Smart Contracts in Move.

Shared assets allow multiple users to operate on them through transactions; that may include some of their owned assets as well as one or more shared assets. These shared assets represent data and logic used to implement protocols that mediate between different users in a safe way, according to the smart contract that defined the type of the shared asset. Sui allows all users to create transactions involving shared assets. But the smart contract type may define additional restrictions on which address and how the shared assets may be used.

A valid transaction submitted to all validators has to be certified and its certificate also has to be submitted to all validators to be finalized. Even if a subset of validators do not follow the protocol, the transaction can be finalized through the remaining validators that correctly follow the Sui protocol. This is achieved through the use of cryptographic Byzantine fault tolerant agreement protocols for broadcast and consensus defined by the Sui protocol. These protocols ensure both safety, meaning that the incorrect validators cannot convince correct clients of incorrect state, and liveness, meaning that incorrect validators cannot prevent transaction processing.

All transactions in Sui have to be associated with a gas asset to cover the cost of processing by Sui. A valid transaction may result in successful execution or an aborted execution. An execution may abort due to a condition within the smart contract defining the asset, or because it has ran out of sufficient gas to pay for the cost of execution. In cases of success, the effects of the operation will be finalized; otherwise, the state of assets in the transaction is not changed. However, the gas asset is always charged some amount of gas, to alleviate denial-of-service attacks on the system as a whole.

A user client can perform the process of submitting the transaction and certificate itself or rely on third party services to submit the transaction and interact with validators. Such third parties need not have user private signature keys and cannot forge transactions on the users' behalf. They can reassure a user client a transaction has been finalized through a set of signatures from validators attesting to the transactions finality and its effects. After that point, the users can be assured that changes the transaction resulted in will persist on the state of Sui.

Sui validators provide facilities for users to read all assets they store, as well as the historical record of transactions they have processed that led to these assets. Validators also provide cryptographic evidence of the full chain of transactions that contributed to an asset state. User clients can request and validate this chain of evidence to ensure all operations were correct and the result of the collective agreement between validators. Services that operate full replicas, mirroring the state of one or more validators, perform such audits routinely.

The public auditability of Sui also implies that all transactions and assets within Sui are publicly visible. Users that are mindful of their privacy may use multiple addresses to benefit from some degree of pseudonymity, or third-party custodial or non-custodial services. Specific smart contracts with additional cryptographic privacy protections can also be provided by third parties.

Sui uses the established Delegated Proof-of Stake model to periodically determine its set of validators. Users can lock and delegate their SUI tokens in each epoch to determine the committee of validators that operate the Sui network in the next epoch. Anyone with over a minimum amount of delegated stake can operate a Sui validator.

Validators operate the network and provide rewards to users that stake their Sui to support them as validators, through gas fee income. Validators with poor reliability, and in turn the users that delegated their stake to them, may receive a lower reward. But user stake cannot be confiscated away either by malicious validators or anyone in the network.

This mechanism ensures that validators are accountable to Sui users and can be rotated out at the first sign of unreliability or misbehavior, including noticed attempts to censor valid transactions. Through choices of validators, and the protocol they are willing to operate, Sui users also have a meaningful say on the future evolution of the Sui system.

If you are looking for an in-depth technical explanation of the computer science behind Sui security, you may have a look at our white paper on the Sui Smart Contracts Platform .

Further reading

If you are looking for an in-depth technical explanation of the computer science behind Sui security, you may have a look at our white paper on the Sui Smart Contracts Platform .