[](https://ida.interchain.io/)

[Interchain Developer Academy](https://ida.interchain.io/)/[Interchain Developer Academy](https://ida.interchain.io/academy/2-cosmos-concepts/2-accounts.html)



Search

[Interchain Developer Academy](https://ida.interchain.io/)[Interchain Developer Academy](https://ida.interchain.io/academy/2-cosmos-concepts/2-accounts.html)

Search



Filters

Interchain Developer Academy

[](https://ida.interchain.io/academy/2-cosmos-concepts/2-accounts.html)

[Week 0 - Getting Started](https://ida.interchain.io/academy/2-cosmos-concepts/2-accounts.html)

[Getting Started](https://ida.interchain.io/academy/2-cosmos-concepts/2-accounts.html)

[Blockchain 101](https://ida.interchain.io/academy/2-cosmos-concepts/2-accounts.html)

[Blockchain History](https://ida.interchain.io/academy/2-cosmos-concepts/2-accounts.html)

[Public and Managed Blockchains](https://ida.interchain.io/academy/2-cosmos-concepts/2-accounts.html)

[Consensus in Distributed Networks](https://ida.interchain.io/academy/2-cosmos-concepts/2-accounts.html)

[Cryptography](https://ida.interchain.io/academy/2-cosmos-concepts/2-accounts.html)

[Self-Assessment Quiz](https://ida.interchain.io/academy/2-cosmos-concepts/2-accounts.html)

[Go Introduction - First Steps](https://ida.interchain.io/academy/2-cosmos-concepts/2-accounts.html)

[Go Basics](https://ida.interchain.io/academy/2-cosmos-concepts/2-accounts.html)

[Go Interfaces](https://ida.interchain.io/academy/2-cosmos-concepts/2-accounts.html)

[Control Structures in Go](https://ida.interchain.io/academy/2-cosmos-concepts/2-accounts.html)

[Arrays and Slices in Go](https://ida.interchain.io/academy/2-cosmos-concepts/2-accounts.html)

[Standard Packages in Go](https://ida.interchain.io/academy/2-cosmos-concepts/2-accounts.html)

[Concurrency in Go](https://ida.interchain.io/academy/2-cosmos-concepts/2-accounts.html)

[Good-To-Know Dev Terms](https://ida.interchain.io/academy/2-cosmos-concepts/2-accounts.html)

[Docker Introduction](https://ida.interchain.io/academy/2-cosmos-concepts/2-accounts.html)

[](https://ida.interchain.io/academy/2-cosmos-concepts/2-accounts.html)

[Week 1 - Introduction to the Interchain](https://ida.interchain.io/academy/2-cosmos-concepts/2-accounts.html)

[Introduction to the Interchain](https://ida.interchain.io/academy/2-cosmos-concepts/2-accounts.html)

[Blockchain Technology and the Interchain](https://ida.interchain.io/academy/2-cosmos-concepts/2-accounts.html)

[The Interchain Ecosystem](https://ida.interchain.io/academy/2-cosmos-concepts/2-accounts.html)

[Getting ATOM and Staking It](https://ida.interchain.io/academy/2-cosmos-concepts/2-accounts.html)

[A Blockchain App Architecture](https://ida.interchain.io/academy/2-cosmos-concepts/2-accounts.html)

[Accounts](https://ida.interchain.io/academy/2-cosmos-concepts/2-accounts.html)

[Transactions](https://ida.interchain.io/academy/2-cosmos-concepts/2-accounts.html)

[Messages](https://ida.interchain.io/academy/2-cosmos-concepts/2-accounts.html)

[Modules](https://ida.interchain.io/academy/2-cosmos-concepts/2-accounts.html)

[Protobuf](https://ida.interchain.io/academy/2-cosmos-concepts/2-accounts.html)

[Multistore and Keepers](https://ida.interchain.io/academy/2-cosmos-concepts/2-accounts.html)

[BaseApp](https://ida.interchain.io/academy/2-cosmos-concepts/2-accounts.html)

[Queries](https://ida.interchain.io/academy/2-cosmos-concepts/2-accounts.html)

[Events](https://ida.interchain.io/academy/2-cosmos-concepts/2-accounts.html)

[Context](https://ida.interchain.io/academy/2-cosmos-concepts/2-accounts.html)

[Testing](https://ida.interchain.io/academy/2-cosmos-concepts/2-accounts.html)

[Relaying with IBC](https://ida.interchain.io/academy/2-cosmos-concepts/2-accounts.html)

[Interchain Security](https://ida.interchain.io/academy/2-cosmos-concepts/2-accounts.html)

[Bridges](https://ida.interchain.io/academy/2-cosmos-concepts/2-accounts.html)

[Migrations](https://ida.interchain.io/academy/2-cosmos-concepts/2-accounts.html)

[Week 1 Quiz](https://ida.interchain.io/academy/2-cosmos-concepts/2-accounts.html)

[](https://ida.interchain.io/academy/2-cosmos-concepts/2-accounts.html)

[Week 2 - First Steps](https://ida.interchain.io/academy/2-cosmos-concepts/2-accounts.html)

[First Steps](https://ida.interchain.io/academy/2-cosmos-concepts/2-accounts.html)

[Setup Your Work Environment](https://ida.interchain.io/academy/2-cosmos-concepts/2-accounts.html)

[Run a Node, API, and CLI](https://ida.interchain.io/academy/2-cosmos-concepts/2-accounts.html)

[Ignite CLI](https://ida.interchain.io/academy/2-cosmos-concepts/2-accounts.html)

[Exercise - Make a Checkers Blockchain](https://ida.interchain.io/academy/2-cosmos-concepts/2-accounts.html)

[Store Object](https://ida.interchain.io/academy/2-cosmos-concepts/2-accounts.html)

[Create Custom Messages](https://ida.interchain.io/academy/2-cosmos-concepts/2-accounts.html)

[Create and Save a Game Properly](https://ida.interchain.io/academy/2-cosmos-concepts/2-accounts.html)

[Add a Way to Make a Move](https://ida.interchain.io/academy/2-cosmos-concepts/2-accounts.html)

[Emit Game Information](https://ida.interchain.io/academy/2-cosmos-concepts/2-accounts.html)

[Record the Game Winner](https://ida.interchain.io/academy/2-cosmos-concepts/2-accounts.html)

[Week 2 Exercise](https://ida.interchain.io/academy/2-cosmos-concepts/2-accounts.html)

[](https://ida.interchain.io/academy/2-cosmos-concepts/2-accounts.html)

[Week 3 - Introduction to IBC and CosmJS](https://ida.interchain.io/academy/2-cosmos-concepts/2-accounts.html)

[Introduction to IBC and CosmJS](https://ida.interchain.io/academy/2-cosmos-concepts/2-accounts.html)

[What is IBC?](https://ida.interchain.io/academy/2-cosmos-concepts/2-accounts.html)

[IBC/TAO - Connections (OPTIONAL)](https://ida.interchain.io/academy/2-cosmos-concepts/2-accounts.html)

[IBC/TAO - Channels (OPTIONAL)](https://ida.interchain.io/academy/2-cosmos-concepts/2-accounts.html)

[IBC/TAO - Clients (OPTIONAL)](https://ida.interchain.io/academy/2-cosmos-concepts/2-accounts.html)

[IBC Token Transfer](https://ida.interchain.io/academy/2-cosmos-concepts/2-accounts.html)

[Interchain Accounts (OPTIONAL)](https://ida.interchain.io/academy/2-cosmos-concepts/2-accounts.html)

[IBC Middleware (OPTIONAL)](https://ida.interchain.io/academy/2-cosmos-concepts/2-accounts.html)

[Create a Custom IBC Middleware (OPTIONAL)](https://ida.interchain.io/academy/2-cosmos-concepts/2-accounts.html)

[Integrate IBC Middleware Into a Chain (OPTIONAL)](https://ida.interchain.io/academy/2-cosmos-concepts/2-accounts.html)

[IBC Tooling](https://ida.interchain.io/academy/2-cosmos-concepts/2-accounts.html)

[What is CosmJS?](https://ida.interchain.io/academy/2-cosmos-concepts/2-accounts.html)

[Your First CosmJS Actions](https://ida.interchain.io/academy/2-cosmos-concepts/2-accounts.html)

[Compose Complex Transactions](https://ida.interchain.io/academy/2-cosmos-concepts/2-accounts.html)

[Learn to Integrate Keplr](https://ida.interchain.io/academy/2-cosmos-concepts/2-accounts.html)

[Create Custom CosmJS Interfaces](https://ida.interchain.io/academy/2-cosmos-concepts/2-accounts.html)

[](https://ida.interchain.io/academy/2-cosmos-concepts/2-accounts.html)

[Week 4 - Ignite CLI and IBC Advanced](https://ida.interchain.io/academy/2-cosmos-concepts/2-accounts.html)

[Ignite CLI and IBC Advanced](https://ida.interchain.io/academy/2-cosmos-concepts/2-accounts.html)

[Keep an Up-To-Date Game Deadline](https://ida.interchain.io/academy/2-cosmos-concepts/2-accounts.html)

[Keep Track Of How Many Moves Have Been Played](https://ida.interchain.io/academy/2-cosmos-concepts/2-accounts.html)

[Put Your Games in Order](https://ida.interchain.io/academy/2-cosmos-concepts/2-accounts.html)

[Auto-Expiring Games](https://ida.interchain.io/academy/2-cosmos-concepts/2-accounts.html)

[Let Players Set a Wager](https://ida.interchain.io/academy/2-cosmos-concepts/2-accounts.html)

[Handle wager payments](https://ida.interchain.io/academy/2-cosmos-concepts/2-accounts.html)

[Integration tests](https://ida.interchain.io/academy/2-cosmos-concepts/2-accounts.html)

[Incentivize Players](https://ida.interchain.io/academy/2-cosmos-concepts/2-accounts.html)

[Help Find a Correct Move](https://ida.interchain.io/academy/2-cosmos-concepts/2-accounts.html)

[Play With Cross-Chain Tokens](https://ida.interchain.io/academy/2-cosmos-concepts/2-accounts.html)

[Understand IBC Denoms](https://ida.interchain.io/academy/2-cosmos-concepts/2-accounts.html)

[Go Relayer](https://ida.interchain.io/academy/2-cosmos-concepts/2-accounts.html)

[Hermes Relayer](https://ida.interchain.io/academy/2-cosmos-concepts/2-accounts.html)

[](https://ida.interchain.io/academy/2-cosmos-concepts/2-accounts.html)

[Week 5 - CosmJS Advanced](https://ida.interchain.io/academy/2-cosmos-concepts/2-accounts.html)

[CosmJS Advanced](https://ida.interchain.io/academy/2-cosmos-concepts/2-accounts.html)

[Create Custom Objects](https://ida.interchain.io/academy/2-cosmos-concepts/2-accounts.html)

[Create Custom Messages](https://ida.interchain.io/academy/2-cosmos-concepts/2-accounts.html)

[Get an External GUI](https://ida.interchain.io/academy/2-cosmos-concepts/2-accounts.html)

[Integrate CosmJS and Keplr](https://ida.interchain.io/academy/2-cosmos-concepts/2-accounts.html)

[Backend Script for Game Indexing](https://ida.interchain.io/academy/2-cosmos-concepts/2-accounts.html)

[](https://ida.interchain.io/academy/2-cosmos-concepts/2-accounts.html)

[Week 6 - IBC Deep Dive](https://ida.interchain.io/academy/2-cosmos-concepts/2-accounts.html)

[IBC Deep Dive](https://ida.interchain.io/academy/2-cosmos-concepts/2-accounts.html)

[IBC Application Developer Introduction](https://ida.interchain.io/academy/2-cosmos-concepts/2-accounts.html)

[Make a Module IBC-Enabled](https://ida.interchain.io/academy/2-cosmos-concepts/2-accounts.html)

[Adding Packet and Acknowledgment Data](https://ida.interchain.io/academy/2-cosmos-concepts/2-accounts.html)

[Extend the Checkers Game With a Leaderboard](https://ida.interchain.io/academy/2-cosmos-concepts/2-accounts.html)

[Create a Leaderboard Chain](https://ida.interchain.io/academy/2-cosmos-concepts/2-accounts.html)

[](https://ida.interchain.io/academy/2-cosmos-concepts/2-accounts.html)

[Week 7 - From Code to MVP to Production and Migrations](https://ida.interchain.io/academy/2-cosmos-concepts/2-accounts.html)

[From Code to MVP to Production and Migrations](https://ida.interchain.io/academy/2-cosmos-concepts/2-accounts.html)

[Run in Production](https://ida.interchain.io/academy/2-cosmos-concepts/2-accounts.html)

[Prepare the Software to Run](https://ida.interchain.io/academy/2-cosmos-concepts/2-accounts.html)

[Prepare a Validator and Keys](https://ida.interchain.io/academy/2-cosmos-concepts/2-accounts.html)

[Prepare Where the Node Starts](https://ida.interchain.io/academy/2-cosmos-concepts/2-accounts.html)

[Prepare and Connect to Other Nodes](https://ida.interchain.io/academy/2-cosmos-concepts/2-accounts.html)

[Configure, Run, and Set Up a Service](https://ida.interchain.io/academy/2-cosmos-concepts/2-accounts.html)

[Prepare and Do Migrations](https://ida.interchain.io/academy/2-cosmos-concepts/2-accounts.html)

[Simulate Production in Docker](https://ida.interchain.io/academy/2-cosmos-concepts/2-accounts.html)

[Tally Player Info After Production](https://ida.interchain.io/academy/2-cosmos-concepts/2-accounts.html)

[Add a Leaderboard as a Module](https://ida.interchain.io/academy/2-cosmos-concepts/2-accounts.html)

[Migrate the Leaderboard Module After Production](https://ida.interchain.io/academy/2-cosmos-concepts/2-accounts.html)

[Simulate a Migration in Docker](https://ida.interchain.io/academy/2-cosmos-concepts/2-accounts.html)

[Final Exam](https://ida.interchain.io/academy/2-cosmos-concepts/2-accounts.html)

[](https://ida.interchain.io/academy/2-cosmos-concepts/2-accounts.html)

[What's Next?](https://ida.interchain.io/academy/2-cosmos-concepts/2-accounts.html)

[Continue Your Interchain Journey](https://ida.interchain.io/academy/2-cosmos-concepts/2-accounts.html)

Docs Version Switcher

On this page

[Public key cryptography](https://ida.interchain.io/academy/2-cosmos-concepts/2-accounts.html#public-key-cryptography)

[Public and private keys](https://ida.interchain.io/academy/2-cosmos-concepts/2-accounts.html#public-and-private-keys)

[Sign and verify](https://ida.interchain.io/academy/2-cosmos-concepts/2-accounts.html#sign-and-verify)

[Hierarchical-deterministic wallets](https://ida.interchain.io/academy/2-cosmos-concepts/2-accounts.html#hierarchical-deterministic-wallets)

[Do I need many addresses?](https://ida.interchain.io/academy/2-cosmos-concepts/2-accounts.html#do-i-need-many-addresses)

[Cryptographic standards](https://ida.interchain.io/academy/2-cosmos-concepts/2-accounts.html#cryptographic-standards)

[Can you be tracked across different addresses?](https://ida.interchain.io/academy/2-cosmos-concepts/2-accounts.html#can-you-be-tracked-across-different-addresses)

[Keyrings, addresses, and address types](https://ida.interchain.io/academy/2-cosmos-concepts/2-accounts.html#keyrings-addresses-and-address-types)

[Signature schemes](https://ida.interchain.io/academy/2-cosmos-concepts/2-accounts.html#signature-schemes)

[Accounts](https://ida.interchain.io/academy/2-cosmos-concepts/2-accounts.html#accounts-2)

[Public keys](https://ida.interchain.io/academy/2-cosmos-concepts/2-accounts.html#public-keys)

[Address](https://ida.interchain.io/academy/2-cosmos-concepts/2-accounts.html#address)

[Keyring](https://ida.interchain.io/academy/2-cosmos-concepts/2-accounts.html#keyring)

[Code example](https://ida.interchain.io/academy/2-cosmos-concepts/2-accounts.html#code-example)

[#Copy link](https://ida.interchain.io/academy/2-cosmos-concepts/2-accounts.html#accounts) **Accounts**



In this section you are going to learn all about accounts in the Interchain:

* What they are
* How they are stored
* Optional implementations
* Cryptography foundations

At the end of the section, you can see how the use of accounts can resolve a current problem for your checkers blockchain: *how to ensure moves are only played by the appropriate player*.

An account is a pair of keys:

* **PubKey:** a public key
* **PrivKey:** a private key

A public key is a unique identifier for a **user or entity** that is safe to disclose. Private keys are sensitive information that users are required to manage confidentially. Private keys are used to sign information in a way that **proves** to others that a message was signed by someone using the private key corresponding to a given public key. This is done without revealing the private key itself.

[#Copy link](https://ida.interchain.io/academy/2-cosmos-concepts/2-accounts.html#public-key-cryptography) Public key cryptography

Modern cryptographic systems leverage computer capabilities to make the power of certain mathematical functions accessible. Public key cryptography is also known as **asymmetric cryptography** and is a cryptographic system that employs pairs of keys. Every pair consists of a public and a private key. The security of the system is not endangered as long as the private key is not disclosed. Compared to symmetric key algorithms, asymmetric ones do not require parties to use a secure channel to exchange the keys for encryption and decryption.

Asymmetric cryptography has two primary applications:

****

**Authentication**

The public key serves as a verification instrument for the private key pair.

****

**Encryption**

Only the private key can decrypt the information encrypted with the public key.

This section focuses on the *authentication* aspect of asymmetric cryptography.



Public key cryptography assures confidentiality, authenticity, and non-repudiation. Examples of applications include [S/MIME (opens new window)↗](https://en.wikipedia.org/wiki/S/MIME) and [GPG (opens new window)↗](https://en.wikipedia.org/wiki/GNU_Privacy_Guard), and it is the basis of several internet standards like [SSL (opens new window)↗](https://www.ssl.com/faqs/faq-what-is-ssl/) and [TLS (opens new window)↗](https://en.wikipedia.org/wiki/Transport_Layer_Security).

Asymmetric cryptography is normally applied to small data blocks due to its computational complexity. Symmetric and asymmetric cryptography can be combined in a hybrid system. For example, asymmetric encryption could be employed to transfer a symmetric encryption, then used as an encryption key for the message. An example of hybrid systems is [PGP (opens new window)↗](https://en.wikipedia.org/wiki/Pretty_Good_Privacy).

The **length of keys** is vital. Asymmetric cryptographic keys are usually very long. One can keep in mind a general principle: the longer the key, the more difficult it is to break the code. Breaking an asymmetric key can only be done with a *brute force attack*, in which an attacker would need to try every possible key to find a match.

[#Copy link](https://ida.interchain.io/academy/2-cosmos-concepts/2-accounts.html#public-and-private-keys) Public and private keys



Asymmetric keys always come in pairs and offer their owner various capabilities. These capabilities are based on cryptographic mathematics. The public key is meant to be distributed to whoever is relevant, while the private key is to remain a secret. This is similar to sharing the address of your house, but keeping the key to your front door private.

[#Copy link](https://ida.interchain.io/academy/2-cosmos-concepts/2-accounts.html#sign-and-verify) Sign and verify

Let's take a look at signing and verifying with public and private keys as an example.

Alice and Bob are communicating. Alice wants to make sure that Bob's public announcement is indeed from Bob, so:

* Bob gives Alice his public key.
* Bob signs his announcement with his private key.
* Bob sends Alice his announcement and its signature.
* Alice verifies the signature with Bob's public key.

Alice can verify the source of the announcement by checking if the signature was done with the private key that corresponds to Bob’s public key (which is already known to represent Bob).



Private keys are used to **prove** that messages originate from the owners of accounts known by their public keys: the signatures **prove** that messages were signed by someone that knows the private key that corresponds to a given public key. This is the basis of user authentication in a blockchain, and why private keys are strictly guarded secrets.

****

**How to manage multiple key pairs over multiple blockchains with hierarchical-deterministic wallets**

[#](https://ida.interchain.io/academy/2-cosmos-concepts/2-accounts.html#hierarchical-deterministic-wallets) **Hierarchical-deterministic wallets**

Blockchains generally maintain ledgers of user accounts and rely on public key cryptography for user authentication. Knowledge of one's public and private keys is a requirement to execute transactions. Client software applications known as wallets provide methods to generate new key pairs and store them, as well as basic services such as creating transactions, signing messages, interacting with applications, and communicating with the blockchain. Although it is technically feasible to generate and store multiple key pairs in a wallet, key management quickly becomes tedious and error-prone for users. Given that all keys would exist only in one place, users would need to devise ways to recover their keys in adverse situations such as the loss or destruction of the computer. The more accounts, the more keys to back up.

[#](https://ida.interchain.io/academy/2-cosmos-concepts/2-accounts.html#do-i-need-many-addresses) Do I need many addresses?

Using multiple addresses can help you improve privacy. You may be a single individual or entity, but you may want to transact with others under different aliases. Additionally, you will likely interact with more than one blockchain in the Interchain Ecosystem. Conveniently, your inevitably-different addresses on different blockchains can all stem from a single seed. A **hierarchical-deterministic wallet** uses a single seed phrase to generate many key pairs to reduce this complexity. Only the seed phrase needs to be backed up.

[#](https://ida.interchain.io/academy/2-cosmos-concepts/2-accounts.html#cryptographic-standards) Cryptographic standards

The Cosmos SDK uses [BIP32 (opens new window)](https://en.bitcoin.it/wiki/BIP_0032), which allows users to generate a set of accounts from an initial **secret** and a **derivation path** containing some input data, such as a blockchain identifier and account index. Since BIP39, this initial secret is mostly generated with 12 or 24 words, known as the mnemonic, taken from a standardized dictionary. Key pairs can always be mathematically reproduced from the mnemonic and the derivation path, which explains the deterministic nature of wallets.

To see BIP32 in action, visit [https://www.bip32.net/ (opens new window)](https://www.bip32.net/).

Click Show entropy details and enter random data in the Entropy field. This reveals an important aspect of the initial seed generation process: a source of randomness is essential. The BIP39 Mnemonic field begins to populate with words as you provide entropy. Scroll down further and select the BIP32 Derivation Path tab. Under Derived Addresses you will see the Public Key and Private Key pairs.

Like most blockchain implementations, the Interchain derives addresses from the public keys.

When using BIP39 or one of its variants, a user is required *only* to store their BIP39 mnemonic in a safe and confidential manner. All key pairs can be reconstructed from the mnemonic because it is deterministic. There is no practical upper limit to the number of key pairs that can be generated from a single mnemonic. The input taken from the [BIP44 (opens new window)](https://github.com/bitcoin/bips/blob/master/bip-0044.mediawiki) derivation path is used to generate a key pair for every blockchain using one single mnemonic. Hence the name "hierarchical-deterministic" to describe this key generation approach.

[#](https://ida.interchain.io/academy/2-cosmos-concepts/2-accounts.html#can-you-be-tracked-across-different-addresses) Can you be tracked across different addresses?

A hierarchical-deterministic wallet also preserves privacy because the next public key or address cannot be deduced from the previous ones. Two addresses issued from a single mnemonic or two addresses created from two different mnemonics are indistinguishable.

[#Copy link](https://ida.interchain.io/academy/2-cosmos-concepts/2-accounts.html#keyrings-addresses-and-address-types) Keyrings, addresses, and address types

In the Cosmos SDK, keys are stored and managed in an object called a **keyring**.

Authentication is implemented as signature verification:

* Users generate transactions, sign transactions, and send signed transactions to the blockchain.
* Transactions are formatted with the public key as part of the message. Signatures are verified by confirming that the signature's public key matches the public key associated with the sender. If the message is signed by anyone other than the purported sender, the signature is invalid and the transaction is rejected.

Consider the following pseudo message in case the foregoing is unclear:



Copy

"Message": {

"Payload": {

"Sender": "0x1234",

"Data": "Hello World"

},

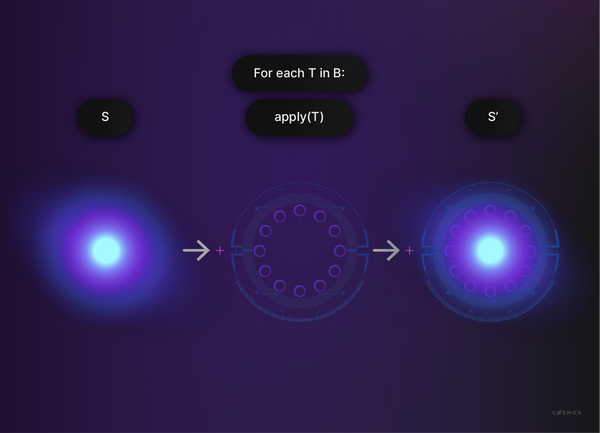
"Signature": "0xabcd"

}

Passing Payload and Signature into the signature verification function returns a sender. The derived sender must match the Sender in the Payload itself. This confirms that the Payload could only originate from someone that knows the private key corresponding to Sender: "0x1234".

[#Copy link](https://ida.interchain.io/academy/2-cosmos-concepts/2-accounts.html#signature-schemes) Signature schemes

There is more than one implementation of the public key signature process previously described. The Cosmos SDK supports the following digital key schemes for creating digital signatures:





The different digital key schemes are implemented in different SDK packages:

* [secp256k1 (opens new window)↗](https://www.secg.org/sec2-v2.pdf), as implemented in the SDK's crypto/keys/secp256k1 package: is the most common and the same one used for Bitcoin.
* [secp256r1 (opens new window)↗](https://www.secg.org/sec2-v2.pdf), as implemented in the SDK's crypto/keys/secp256r1 package.
* [tm-ed25519 (opens new window)↗](https://ed25519.cr.yp.to/ed25519-20110926.pdf), as implemented in the SDK's crypto/keys/ed25519 package: is supported only for consensus validation.

[#Copy link](https://ida.interchain.io/academy/2-cosmos-concepts/2-accounts.html#accounts-2) Accounts

The [BaseAccount (opens new window)↗](https://github.com/cosmos/cosmos-sdk/blob/bf11b1bf1fa0c52fb2cd51e4f4ab0c90a4dd38a0/x/auth/types/auth.pb.go#L31-L36) object provides the basic account implementation that stores authentication information.

[#Copy link](https://ida.interchain.io/academy/2-cosmos-concepts/2-accounts.html#public-keys) Public keys

Public keys are generally not used to reference accounts (see the following section, *Address*). Public keys do exist and they are accessible through the [cryptoTypes.PubKey (opens new window)↗](https://github.com/cosmos/cosmos-sdk/blob/9fd866e3820b3510010ae172b682d71594cd8c14/crypto/types/types.go#L9) interface. This facilitates operations which developers may find useful, such as signing off-chain messages or using a public key for other out-of-band operations.

[#Copy link](https://ida.interchain.io/academy/2-cosmos-concepts/2-accounts.html#address) Address

An address is public information normally used to reference an account. Addresses are derived from public keys using [ADR-28 (opens new window)↗](https://github.com/cosmos/cosmos-sdk/blob/master/docs/architecture/adr-028-public-key-addresses.md). Three types of addresses specify a context when an account is used:

* [AccAddress (opens new window)↗](https://github.com/cosmos/cosmos-sdk/blob/1dba6735739e9b4556267339f0b67eaec9c609ef/types/address.go#L129) identifies users, which are the sender of a message.
* [ValAddress (opens new window)↗](https://github.com/cosmos/cosmos-sdk/blob/23e864bc987e61af84763d9a3e531707f9dfbc84/types/address.go#L298) identifies validator operators.
* [ConsAddress (opens new window)↗](https://github.com/cosmos/cosmos-sdk/blob/23e864bc987e61af84763d9a3e531707f9dfbc84/types/address.go#L448) identifies validator nodes that are participating in consensus. Validator nodes are derived using the [ed25519 (opens new window)↗](https://www.cryptosys.net/pki/manpki/pki_eccsafecurves.html) curve.

[#Copy link](https://ida.interchain.io/academy/2-cosmos-concepts/2-accounts.html#keyring) Keyring

The keyring object stores and manages multiple accounts. The keyring object implements the [Keyring (opens new window)↗](https://github.com/cosmos/cosmos-sdk/blob/bf11b1bf1fa0c52fb2cd51e4f4ab0c90a4dd38a0/crypto/keyring/keyring.go#L55) interface in the Cosmos SDK.

[#Copy link](https://ida.interchain.io/academy/2-cosmos-concepts/2-accounts.html#code-example) Code example

****

**Show me some code for my checkers blockchain**

In the [previous section](https://ida.interchain.io/academy/2-cosmos-concepts/1-architecture.html), your ABCI application accepted anonymous checkers moves. This is a problem. With accounts, you can restrict moves to the right player.   
  
It is necessary to differentiate between players and other actors. This helps assure there is no identity spoofing, that players do not play out of turn, and rewards are paid to the correct winner. You are also going to store the creator of a game, which may or may not be a player.   
  
**Game object**

First define some elements of the eventual stored game:



Copy

type StoredGame struct {

Creator string // A stringified address for the creator of the game.

Black string // A stringified address for the player playing blacks.

Red string // A stringified address for the player playing reds.

...

}

How would you extract and serialize addresses? Handle the extraction like this:



Copy

import (

sdk "github.com/cosmos/cosmos-sdk/types"

)

creator, err := sdk.AccAddressFromBech32(storedGame.Creator)

if err != nil {

// Handle the error.

}

Handle the serialization as follows:



Copy

var creator sdk.AccAddress

storedGame.Creator = creator.String()

With these snippets, you will be able to accept only the right players when it comes to transactions.   
  
**Remaining game object**

Defining the players is good, but the stored game is not complete unless you add game details like the current board state and the game's unique identifier. Conveniently, you can [serialize (opens new window)↗](https://github.com/batkinson/checkers-go/blob/a09daeb/checkers/checkers.go#L303) and [deserialize (opens new window)↗](https://github.com/batkinson/checkers-go/blob/a09daeb/checkers/checkers.go#L331) the board state. You can already confirm the following struct:



Copy

type StoredGame struct {

Creator string

Index string // The unique id that identifies this game.

Board string // The serialized board.

Turn string // "black" or "red"

Black string

Red string

}



If you want to go beyond the out-of-context code samples above and instead see more details on defining this, head to [Run Your Own Chain](https://ida.interchain.io/hands-on-exercise/1-ignite-cli/).

synopsis

To summarize, this section has explored:

* How an account consists of a public key (a unique account identifier which is safe to disclose) and a private key (a corresponding signature tool which must be kept confidential by the account holder).
* How public private key pairs are used to sign and verify communications, forming the basis of user authentication in a blockchain.
* How hierarchical-deterministic wallets provide a convenient way to generate and store key pairs and perform various basic activities such as creating transactions, signing messages, interacting with applications, and communicating with the blockchain.
* How the Interchain uses the BIP32 cryptographic standard, and the employment of mnemonics as a means of securing a user's wallet.
* The use of the keyring object for storing and managing keys, and the digital key schemes which are used by different SDK packages.
* The three types of address which identify users, validator operators, and validator nodes.

previous

[](https://ida.interchain.io/academy/2-cosmos-concepts/1-architecture.html)

**[A Blockchain App Architecture](https://ida.interchain.io/academy/2-cosmos-concepts/1-architecture.html)**

up next

**[Transactions](https://ida.interchain.io/academy/2-cosmos-concepts/3-transactions.html)**

[[](https://ida.interchain.io/academy/2-cosmos-concepts/3-transactions.html)](https://ida.interchain.io/academy/2-cosmos-concepts/3-transactions.html)

Rate this Page

icon smile

icon meh

icon frown

Would you like to add a message?

Submit

Thank you for your Feedback!

[](https://ida.interchain.io/ida-course/discord-info.html)

On this page

[Public key cryptography](https://ida.interchain.io/academy/2-cosmos-concepts/2-accounts.html#public-key-cryptography)

[Public and private keys](https://ida.interchain.io/academy/2-cosmos-concepts/2-accounts.html#public-and-private-keys)

[Sign and verify](https://ida.interchain.io/academy/2-cosmos-concepts/2-accounts.html#sign-and-verify)

[Hierarchical-deterministic wallets](https://ida.interchain.io/academy/2-cosmos-concepts/2-accounts.html#hierarchical-deterministic-wallets)

[Do I need many addresses?](https://ida.interchain.io/academy/2-cosmos-concepts/2-accounts.html#do-i-need-many-addresses)

[Cryptographic standards](https://ida.interchain.io/academy/2-cosmos-concepts/2-accounts.html#cryptographic-standards)

[Can you be tracked across different addresses?](https://ida.interchain.io/academy/2-cosmos-concepts/2-accounts.html#can-you-be-tracked-across-different-addresses)

[Keyrings, addresses, and address types](https://ida.interchain.io/academy/2-cosmos-concepts/2-accounts.html#keyrings-addresses-and-address-types)

[Signature schemes](https://ida.interchain.io/academy/2-cosmos-concepts/2-accounts.html#signature-schemes)

[Accounts](https://ida.interchain.io/academy/2-cosmos-concepts/2-accounts.html#accounts-2)

[Public keys](https://ida.interchain.io/academy/2-cosmos-concepts/2-accounts.html#public-keys)

[Address](https://ida.interchain.io/academy/2-cosmos-concepts/2-accounts.html#address)

[Keyring](https://ida.interchain.io/academy/2-cosmos-concepts/2-accounts.html#keyring)

[Code example](https://ida.interchain.io/academy/2-cosmos-concepts/2-accounts.html#code-example)

#### **Get Cosmos updates**

Unsubscribe at any time. [Privacy Policy↗](https://v1.cosmos.network/privacy)

     Next

Documentation

[Cosmos SDK](https://docs.cosmos.network/)[Cosmos Hub](https://hub.cosmos.network/)[CometBFT](https://docs.cometbft.com/)[IBC Protocol](https://ibc.cosmos.network/)

Community

[Interchain blog](https://blog.cosmos.network/)[Forum](https://forum.cosmos.network/)[Discord](https://discord.gg/cosmosnetwork)

Contributing

[Source code on GitHub](https://github.com/cosmos/sdk-tutorials)

[](https://ida.interchain.io/)

[Interchain Developer Academy](https://ida.interchain.io/)

**[](https://blog.cosmos.network/)[](https://twitter.com/cosmos)[](https://discord.gg/cosmosnetwork)[](https://www.linkedin.com/company/interchain-foundation/about/)[](https://reddit.com/r/cosmosnetwork)[](https://t.me/cosmosproject)[](https://www.youtube.com/c/CosmosProject)**



Dark mode

† This website is maintained by the Interchain Foundation (ICF). The contents and opinions of this website are those of the ICF. The ICF provides links to cryptocurrency exchanges as a service to the public. The ICF does not warrant that the information provided by these websites is correct, complete, and up-to-date. The ICF is not responsible for their content and expressly rejects any liability for damages of any kind resulting from the use, reference to, or reliance on any information contained within these websites.

Cosmos is a registered trademark of the [Interchain Foundation.](https://interchain.io/)[Privacy](https://v1.cosmos.network/privacy)