Pact Language Reference Documentation

Release 2.2.2

Stuart Popejoy

Jul 17, 2017

Contents

Contents:

This document is a reference for the Pact smart-contract language, designed for correct, transactional execution on a high-performance blockchain. For more background, please see the white paper or the pact home page.

CHAPTER 1

Changelog

Version 2.2.2:

- Module Hashes: `use` support
- use accepts barewords
- better output in `describe-module`
- `list-modules` added
- `print` REPL command
- "transactional awareness" in Persist

Version 2.2.1:

- `yield` and `resume` added for use in defpacts
- `yielded`, `sig-keyset` repl functions
- JSON defaults for keysets, better dispatch of builtin preds
- `pact-version` function added.

Version 2.2.0:

- Privacy API: `private` endpoint, address fields in command
- Typechecker support for `at`,`filter`,`map`,`fold`,`compose`
- Persist layer standardized for easier extension
- Library features: Interpreter module, NFData all the things, Eval uses exceptions
- Types module breakup

Version 2.1.0:

- "pact -serve": new REST API server for app development
- pact-lang-api.js javascript package
- `json` repl function, `read-msg` can take zero args to get entire data payload

Version 2.0:

- Types and schemas added
- `with-keyset` changed to non-special-form `enforce-keyset`
- Table definitions added; database functions reference these directly instead of using strings.

CHAPTER 2

Rest API

As of version 2.1.0 Pact ships with a built-in HTTP server and SQLite backend. This allows for prototyping blockchain applications with just the `pact` tool.

To start up the server issue `pact -s config.yaml`, with a suitable config. The `pact-lang-api` JS library is available via npm for web development.

load.js

The `load.js` tool can be used to format valid `send` and `private` payloads for use with a POST tool like Postman or even piping into `curl`.

```
$ ./load.js
ERROR: Missing code or codefile argument

load.js: create JSON for loading Pact code

Arguments: [-cf codefile] [-c code] -n nonce -s sk -p pk [-df datafile] [-d data] [-t␣
↪to -f from]

  codefile    filepath containing pact code to load
  code        pact code to execute
  datafile    filepath containing JSON data to accompany pact code load
  data        JSON string of data to accompany pact code load
  nonce       nonce value for data payload
  sk          secret key
  pk          public key
  to          Private message sender entity
  from        Private message recipient JSON list

$ ./load.js -c "(cash.read-account \"will\")" -df ../tests/cp-auth-keys.json -n "hello
↪" -s 236270aa77997037db05201978775ea157392bed858b36ec0edf8444f6a52983 -p␣
↪e6f65edd34986745f1d3a4a3f9706ad35a0049005d63117578a800701c9ef8cc -f Me -t "[\"You\",
↪\"Him\",\"Her\"]"
```

```
{"cmds":[{"hash":
↪"3c4038053663af50a0851e8e4987f50c6147e3a1cecbce46fd6e14c04496d5ff731d6d980c9733743bb11488996e23567
↪","sigs":[{"sig":
↪"587dd0972cd271d828d1b12319f8f3c2a42631b64b3f331bc0091b4f7cf0b98f20a8e3e5dd056e7fe08fe3981d24b11e4
↪","pubKey":"e6f65edd34986745f1d3a4a3f9706ad35a0049005d63117578a800701c9ef8cc"}],"cmd
↪":"{\"nonce\":\"hello\",\"payload\":{\"exec\":{\"code\":\"(cash.read-account \\\
↪"will\\\")\",\"data\":{\"module-admin-keyset\":{\"keys\":[\
↪"e6f65edd34986745f1d3a4a3f9706ad35a0049005d63117578a800701c9ef8cc\"],\"pred\":\
↪"keys-all\"}}}},\"address\":{\"from\":\"Me\",\"to\":[\"You\",\"Him\",\"Her\"]}}"}]}
```

Endpoints

All endpoints are served from `api/v1`. Thus a `send` call would be sent to (http://localhost:8080/api/v1/send){[}http://localhost:8080/api/v1/send], if running on `localhost:8080`.

send

Asynchronous submit of one or more *public* (unencrypted) commands to the blockchain.

Request JSON:

```
{
  "cmds": [
  { \\ "Command" JSON
    "hash": "[blake2 hash in base16 of 'cmd' value]",
    "sigs": [
      {
        "sig": "[crypto signature by secret key of 'hash' value]",
        "pubKey": "[base16-format of public key of signing keypair]",
        "scheme": "ED25519" /* optional field, defaults to ED25519, will support␣
↪other curves as needed */
      }
    ]
    "cmd": {
      "nonce": "[nonce value]",
      "payload": {
        "exec": "[pact code]",
        "data": {
          /* arbitrary user data to accompany code */
        }
      }
    }
  } \\ end "Command" JSON
}
```

Response JSON:

```
{
  "status": "success|failure",
  "response": {
    "requestKeys": [
      "[matches hash from each sent/processed command, use with /poll or /listen to␣
↪get tx results]"
    ]
```

```
  }
}
```

private

Asynchronous submit of one or more *private* commands to the blockchain, using supplied address info to securely encrypt for only sending and receiving entities to read.

Request JSON:

```
{
  "cmds": [
  { \\ "Command" JSON
    "hash": "[blake2 hash in base16 of 'cmd' value]",
    "sigs": [
      {
        "sig": "[crypto signature by secret key of 'hash' value]",
        "pubKey": "[base16-format of public key of signing keypair]",
        "scheme": "ED25519" /* optional field, defaults to ED25519, will support␣
↪other curves as needed */
      }
    ]
    "cmd": {
      "address": {
        "from": "[Sending entity name, must match sending entity node entity name]",
        "to": ["A","B"] /* list of recipient entity names */
      }
      "nonce": "[nonce value]"
      "payload": {
        "exec": "[pact code]",
        "data": {
          /* arbitrary user data to accompany code */
        }
      }
    }
  } \\ end "Command" JSON
}
```

Response JSON:

```
{
  "status": "success|failure",
  "response": {
    "requestKeys": [
      "[matches hash from each sent/processed command, use with /poll or /listen to␣
↪get tx results]"
    ]
  }
}
```

poll

Poll for command results.

Request JSON:

```
{
  "requestKeys": [
    "[hash from desired commands to poll]"
  ]
}
```

Response JSON:

```
{
  "status": "success|failure",
  "response": {
    "[command hash]": {
      "result": {
        "status": "success|failure",
        "data": /* data from Pact execution represented as JSON */
      },
      "txId": /* integer transaction id, for use in querying history etc */
    }
  }
}
```

listen

Blocking call to listen for a single command result, or retrieve an already-executed command.

Request JSON:

```
{
  "listen": "[command hash]"
}
```

Response JSON:

```
{
  "status": "success|failure",
  "response": {
    "result": {
      "status": "success|failure",
      "data": /* data from Pact execution represented as JSON */
    },
    "txId": /* integer transaction id, for use in querying history etc */
  }
}
```

local

Blocking/sync call to send a command for non-transactional execution. In a blockchain environment this would be a node-local "dirty read". Any database writes or changes to the environment are rolled back.

Request JSON:

```
{ \\ "Command" JSON
  "hash": "[blake2 hash in base16 of 'cmd' value]",
  "sigs": [
    {
```

```
      "sig": "[crypto signature by secret key of 'hash' value]",
      "pubKey": "[base16-format of public key of signing keypair]",
      "scheme": "ED25519" /* optional field, defaults to ED25519, will support other␣
↪curves as needed */
    }
  ]
  "cmd": {
    "nonce": "[nonce value]",
    "payload": {
      "exec": "[pact code]",
      "data": {
        /* arbitrary user data to accompany code */
      }
    }
  }
} \\ end "Command" JSON
```

Response JSON:

```
{
  "status": "success|failure",
  "response": {
    "status": "success|failure",
    "data": /* data from Pact execution represented as JSON */
  }
}
```

CHAPTER 3

Concepts

Execution Modes

Pact is designed to be used in distinct *execution modes* to address the performance requirements of rapid linear execution on a blockchain. These are:

1. Contract definition.
2. Transaction execution.
3. Queries and local execution.

Contract Definition

In this mode, a large amount of code is sent into the blockchain to establish the smart contract, as comprised of code (modules), tables (data), and keysets (authorization). This can also include "transactional" (database-modifying) code, for instance to initialize data.

For a given smart contract, these should all be sent as a single message into the blockchain, so that any error will rollback the entire smart contract as a unit.

Keyset definition

Keysets are customarily defined first, as they are used to specify admin authorization schemes for modules and tables. Definition creates the keysets in the runtime environment and stores their definition in the global keyset database.

Module declaration

Modules contain the API and data definitions for smart contracts. They are comprised of:

- *functions*
- *schema* definitions

- *table* definitions
- *"pact"* special functions
- *const* values

When a module is declared, all references to native functions or definitions from other modules are resolved. Resolution failure results in transaction rollback.

Modules can be re-defined as controlled by their admin keyset. Module versioning is not supported, except by including a version sigil in the module name (e.g., "accounts-v1"). However, *module hashes* are a powerful feature for ensuring code safety. When a module is imported with *use*, the module hash can be specified, to tie code to a particular release.

As of Pact 2.2, `use` statements can be issued within a module declaration. This combined with module hashes provides a high level of assurance, as updated module code will fail to import if a dependent module has subsequently changed on the chain; this will also propagate changes to the loaded modules' hash, protecting downstream modules from inadvertent changes on update.

Module names must be globally unique.

Table Creation

Tables are *created* at the same time as modules. While tables are *defined* in modules, they are *created* "after" modules, so that the module may be redefined later without having to necessarily re-create the table.

The relationship of modules to tables is important, as described in *Table Guards*.

There is no restriction on how many tables may be created. Table names are namespaced with the module name.

Tables can be typed with a *schema*.

Transaction Execution

"Transactions" refer to business events enacted on the blockchain, like a payment, a sale, or a workflow step of a complex contractual agreement. A transaction is generally a single call to a module function. However there is no limit on how many statements can be executed. Indeed, the difference between "transactions" and "smart contract definition" is simply the *kind* of code executed, not any actual difference in the code evaluation.

Queries and Local Execution

Querying data is generally not a business event, and can involve data payloads that could impact performance, so querying is carried out as a *local execution* on the node receiving the message. Historical queries use a *transaction ID* as a point of reference, to avoid any race conditions and allow asynchronous query execution.

Transactional vs local execution is accomplished by targeting different API endpoints; pact code has no ability to distinguish between transactional and local execution.

Database Interaction

Pact presents a database metaphor reflecting the unique requirements of blockchain execution, which can be adapted to run on different back-ends.

Atomic execution

A single message sent into the blockchain to be evaluated by Pact is *atomic*: the transaction succeeds as a unit, or does not succeed at all, known as "transactions" in database literature. There is no explicit support for rollback handling, except in *multi-step transactions*.

Key-Row Model

Blockchain execution can be likened to OLTP (online transaction processing) database workloads, which favor denormalized data written to a single table. Pact's data-access API reflects this by presenting a *key-row* model, where a row of column values is accessed by a single key.

As a result, Pact does not support *joining* tables, which is more suited for an OLAP (online analytical processing) database, populated from exports from the Pact database. This does not mean Pact cannot *record* transactions using relational techniques – for example, a Customer table whose keys are used in a Sales table would involve the code looking up the Customer record before writing to the Sales table.

No Nulls

Pact has no concept of a NULL value in its database metaphor. The main function for computing on database results, *with-read*, will error if any column value is not found. Authors must ensure that values are present for any transactional read. This is a safety feature to ensure *totality* and avoid needless, unsafe control-flow surrounding null values.

Versioned History

The key-row model is augmented by every change to column values being versioned by transaction ID. For example, a table with three columns "name", "age", and "role" might update "name" in transaction #1, and "age" and "role" in transaction #2. Retreiving historical data will return just the change to "name" under transaction 1, and the change to "age" and "role" in transaction #2.

Back-ends

Pact guarantees identical, correct execution at the smart-contract layer within the blockchain. As a result, the backing store need not be identical on different consensus nodes. Pact's implementation allows for integration of industrial RDBMSs, to assist large migrations onto a blockchain-based system, by facilitating bulk replication of data to downstream systems.

Types and Schemas

With Pact 2.0, Pact gains explicit type specification, albeit optional. Pact 1.0 code without types still functions as before, and writing code without types is attractive for rapid prototyping.

Schemas provide the main impetus for types. A schema *is defined* with a list of columns that can have types (although this is also not required). Tables are then *defined* with a particular schema (again, optional).

Note that schemas also can be used on/specified for object types.

Runtime Type enforcement

Any types declared in code are enforced at runtime. For table schemas, this means any write to a table will be typechecked against the schema. Otherwise, if a type specification is encountered, the runtime enforces the type when the expression is evaluated.

Static Type Inference on Modules

With the *typecheck* repl command, the Pact interpreter will analyze a module and attempt to infer types on every variable, function application or const definition. Using this in project repl scripts is helpful to aid the developer in adding "just enough types" to make the typecheck succeed. Fully successful typecheck is usually a matter of providing schemas for all tables, and argument types for ancilliary functions that call ambigious or overloaded native functions.

Formal Verification

Pact's typechecker is designed to output a fully typechecked, inlined AST for use generating formal proofs in SMT-LIB2. If the typecheck does not fully succeed, the module is not considered "provable".

We see, then, that Pact code can move its way up a "safety" gradient, starting with no types, then with "enough" types, and lastly, with formal proofs.

Note that as of Pact 2.0 the formal verification function is still under development.

Keysets and Authorization

Pact is inspired by Bitcoin scripts to incorporate public-key authorization directly into smart contract execution and administration.

Keyset definition

Keysets are *defined* by *reading* definitions from the message payload. Keysets consist of a list of public keys and a *keyset predicate*.

Examples of valid keyset JSON productions:

```
/* examples of valid keysets */
{
  "fully-specified":
    { "keys": ["abc6bab9b88e08d","fe04ddd404feac2"], "pred": "keys-2" }

  "keysonly":
    { "keys": ["abc6bab9b88e08d","fe04ddd404feac2"] } /* defaults to "keys-all" pred␣
↪*/

  "keylist": ["abc6bab9b88e08d","fe04ddd404feac2"] /* makes a "keys-all" pred keyset␣
↪*/
}
```

Keyset Predicates

A keyset predicate references a function by name which will compare the public keys in the keyset to the key or keys used to sign the blockchain message. The function accepts two arguments, "count" and "matched", where "count" is the number of keys in the keyset and "matched" is how many keys on the message signature matched a keyset key.

Support for multiple signatures is the responsibility of the blockchain layer, and is a powerful feature for Bitcoin-style "multisig" contracts (ie requiring at least two signatures to release funds).

Pact comes with built-in keyset predicates: *keys-all*, *keys-any*, *keys-2*. Module authors are free to define additional predicates.

If a keyset predicate is not specified, it is defaulted to *keys-all*.

Key rotation

Keysets can be rotated, but only by messages authorized against the current keyset definition and predicate. Once authorized, the keyset can be easily *redefined*.

Module Table Guards

When *creating* a table, a module name must also be specified. By this mechanism, tables are "guarded" or "encapsulated" by the module, such that direct access to the table via *data-access functions* is authorized by the module's admin keyset. However, *within module functions*, table access is unconstrained. This gives contract authors great flexibility in designing data access, and is intended to enshrine the module as the main "user" data access API.

Row-level keysets

Keysets can be stored as a column value in a row, allowing for *row-level* authorization. The following code indicates how this might be achieved:

```
(defun create-account (id)
  (insert accounts id { "balance": 0.0, "keyset": (read-keyset "owner-keyset") }))

(defun read-balance (id)
  (with-read { "balance":= bal, "keyset":= ks }
    (enforce-keyset ks)
    (format "Your balance is {}" bal)))
```

In the example, `create-account` reads a keyset definition from the message payload using *read-keyset* to store as "keyset" in the table. `read-balance` only allows that owner's keyset to read the balance, by first enforcing the keyset using *enforce-keyset*.

Computational Model

Here we cover various aspects of Pact's approach to computation.

Turing-Incomplete

Pact is turing-incomplete, in that there is no recursion (recursion is detected before execution and results in an error) and no ability to loop indefinitely. Pact does support operation on list structures via *map*, *fold* and *filter*, but since there is no ability to define infinite lists, these are necessarily bounded.

Turing-incompleteness allows Pact module loading to resolve all references in advance, meaning that instead of addressing functions in a lookup table, the function definition is directly injected (or "inlined") into the callsite. This is an example of the performance advantages of a Turing-incomplete language.

Single-assignment Variables

Pact allows variable declarations in *let expressions* and *bindings*. Variables are immutable: they cannot be re-assigned, or modified in-place.

A common variable declaration occurs in the *with-read* function, assigning variables to column values by name. The *bind* function offers this same functionality for objects.

Module-global constant values can be declared with *defconst*.

Data Types

Pact code can be explicitly typed, and is always strongly-typed under the hood as the native functions perform strict typechecking as indicated in their documented type signatures. language, but does use fixed type representations "under the hood" and does no coercion of types, so is strongly-typed nonetheless.

Pact's supported types are:

- *Strings*
- *Integers*
- *Decimals*
- *Booleans*
- *Key sets*
- *Lists*
- *Objects*
- *Function* and *pact* definitions
- *JSON values*
- *Tables*
- *Schemas*

Performance

Pact is designed to maximize the performance of *transaction execution*, penalizing queries and module definition in favor of fast recording of business events on the blockchain. Some tips for fast execution are:

Single-function transactions

Design transactions so they can be executed with a single function call.

Call with references instead of `use`

When calling module functions in transactions, use *reference syntax* instead of importing the module with *use*. When defining modules that reference other module functions, `use` is fine, as those references will be inlined at module definition time.

Hardcoded arguments vs. message values

A transaction can encode values directly into the transactional code:

```
(accounts.transfer "Acct1" "Acct2" 100.00)
```

or it can read values from the message JSON payload:

```
(defun transfer-msg ()
  (transfer (read-msg "from") (read-msg "to")
            (read-decimal "amount")))
...
(accounts.transfer-msg)
```

The latter will execute slightly faster, as there is less code to interpret at transaction time.

Types as necessary

With table schemas, Pact will be strongly typed for most use cases, but functions that do not use the database might still need types. Use the typecheck REPL function to add the necessary types. There is a small cost for type enforcement at runtime, and too many type signatures can harm readability. However types can help document an API, so this is a judgement call.

Control Flow

Pact supports conditionals via *if*, bounded looping, and of course function application.

"If" considered harmful

Consider avoiding `if` wherever possible: every branch makes code harder to understand and more prone to bugs. The best practice is to put "what am I doing" code in the front-end, and "validate this transaction which I intend to succeed" code in the smart contract.

Pact's original design left out `if` altogether (and looping), but it was decided that users should be able to judiciously use these features as necessary.

Use enforce

"If" should never be used to enforce business logic invariants: instead, *enforce* is the right choice, which will fail the transaction.

Indeed, failure is the only *non-local exit* allowed by Pact. This reflects Pact's emphasis on *totality*.

Use built-in keysets

The built-in keyset functions *keys-all*, *keys-any*, *keys-2* are hardcoded in the interpreter to execute quickly. Custom keysets require runtime resolution which is slower.

Functional Concepts

Pact includes the functional-programming "greatest hits": *map*, *fold* and *filter*. These all employ *partial application*, where the list item is appended onto the application arguments in order to serially execute the function.

```
(map (+ 2) [1 2 3])
(fold (+) ["Concatenate" " " "me"]
```

Pact also has *compose*, which allows "chaining" applications in a functional style.

LISP

Pact's use of LISP syntax is intended to make the code reflect its runtime representation directly, allowing contract authors focus directly on program execution. Pact code is stored in human-readable form on the ledger, such that the code can be directly verified, but the use of LISP-style *s-expression syntax* allows this code to execute quickly.

Message Data

Pact expects code to arrive in a message with a JSON payload and signatures. Message data is read using *read-msg* and related functions, while signatures are not directly readable or writable – they are evaluated as part of *keyset predicate* enforcement.

JSON support

Values returned from Pact transactions are expected to be directly represented as JSON values.

When reading values from a message via *read-msg*, Pact coerces JSON types as follows:

- String -> String
- Number -> Integer (rounded)
- Boolean -> Boolean
- Object -> JSON Value
- Array -> JSON Value
- Null -> JSON Value

Decimal values are represented as Strings and read using *read-decimal*.

JSON Objects, Arrays, and Nulls are not coerced, intended for direct storage and retreival as opaque payloads in the database.

Confidentiality

Pact is designed to be used in a *confidentiality-preserving* environment, where messages are only visible to a subset of participants. This has significant implications for smart contract execution.

Entities

An *entity* is a business participant that is able or not able to see a confidential message. An entity might be a company, a group within a company, or an individual.

Disjoint Databases

Pact smart contracts operate on messages organized by a blockchain, and serve to produce a database of record, containing results of transactional executions. In a confidential environment, different entities execute different transactions, meaning the resulting databases are now *disjoint*.

This does not affect Pact execution; however, database data can no longer enact a "two-sided transaction", meaning we need a new concept to handle enacting a single transaction over multiple disjoint datasets.

Pacts

Pacts are multi-step sequential transactions that are defined as a single body of code called a *pact*. With a pact, participants ensure they are executing an identical code path, even as they execute distinct "steps" in that path.

The concept of pacts reflect *coroutines* in software engineering: functions that can *yield* and *resume* computation "in the middle of" their body. A *step* in a pact designates a target entity to execute it, after which the pact "yields" execution, completing the transaction and initiating a signed "Resume" message into the blockchain.

The function *yield* and special form *resume* allow for passing computed values between subsequent steps. These are not available for rollback functions however.

The counterparty entity sees this "Resume" message and drops back into the pact body to find if the next step is targetted for it, if so executing it.

Since any step can fail, steps can be designed with *rollbacks* to undo changes if a subsequent step fails.

Note that at this time, it is not possible to simulate multi-party defpact executions in the pact server environment, as this is necessarily a multi-node/multi-entity interaction. Pacts can be tested in repl scripts using the *env-entity*, *env-step* and *yielded* repl functions to simulate multi-entity interactions.

CHAPTER 4

Syntax

Literals

Strings

String literals are created with double-ticks:

```
pact> "a string"
"a string"
```

Strings also support multiline by putting a backslash before and after whitespace (not interactively).

```
(defun id (a)
  "Identity function. \
  \Argument is returned."
  a)
```

Symbols

Symbols are string literals representing some unique item in the runtime, like a function or a table name. Their representation internally is simply a string literal so their usage is idiomatic.

Symbols are created with a preceding tick, thus they do no support whitespace or multiline.

```
pact> 'a-symbol
"a-symbol"
```

Integers

Integer literals are unbounded positive naturals. For negative numbers use the unary - function.

```
pact> 12345
12345
```

Decimals

Decimal literals are positive decimals to exact expressed precision.

```
pact> 100.25
100.25
pact> 356452.23451872
356452.23451872
```

Booleans

Booleans are represented by `true` and `false` literals.

```
pact> (and true false)
false
```

Lists

List literals are created with brackets. Uniform literal lists are given a type in parsing.

```
pact> [1 2 3]
[1 2 3]
pact> (typeof [1 2 3])
"[integer]"
pact> (typeof [1 2 true])
"list"
```

Objects

Objects are dictionaries, created with curly-braces specifying key-value pairs using a colon `:`. For certain applications (database updates), keys must be strings.

```
pact> { "foo": (+ 1 2), "bar": "baz" }
(TObject [("foo",3),("bar","baz")])
```

Bindings

Bindings are dictionary-like forms, also created with curly braces, to bind database results to variables using the `:=` operator. They are used in *with-read*, *with-default-read*, *bind* and *resume* to assign variables to named columns in a row, or values in an object.

```
(defun check-balance (id)
  (with-read accounts id { "balance" := bal }
    (enforce (> bal 0) (format "Account in overdraft: {}" bal))))
```

Type specifiers

Types can be specified in syntax with the colon `:` operator followed by a type literal or user type specification.

Type literals

- `string`
- `integer`
- `decimal`
- `bool`
- `keyset`
- `list`, or `[type]` to specify the list type
- `object`, which can be further typed with a schema
- `table`, which can be further typed with a schema
- `value` (JSON values)

Schema type literals

A schema defined with *defschema* is referenced by name enclosed in curly braces.

```
table:{accounts}
object:{person}
```

What can be typed

Function arguments and return types

```
(defun prefix:string (pfx:string str:string) (+ pfx str))
```

Let variables

```
(let ((a:integer 1) (b:integer 2)) (+ a b))
```

Tables and objects

Tables and objects can only take a schema type literal.

```
(deftable accounts:{account})

(defun get-order:{order} (id) (read orders id))
```

Consts

```
(defconst PENNY:decimal 0.1)
```

Special forms

defun

```
(defun NAME ARGLIST [DOCSTRING] BODY...)
```

Define NAME as a function, accepting ARGLIST arguments, with optional DOCSTRING. Arguments are in scope for BODY, one or more expressions.

```
(defun add3 (a b c) (+ a (+ b c)))

(defun scale3 (a b c s) "multiply sum of A B C times s"
  (* s (add3 a b c)))
```

defconst

```
(defun NAME VALUE [DOCSTRING])
```

Define NAME as VALUE, with option DOCSTRING.

```
(defconst COLOR_RED="#FF0000" "Red in hex")
(defconst COLOR_GRN="#00FF00" "Green in hex")
(defconst PI 3.14159265 "Pi to 8 decimals")
```

defpact

```
(defpact NAME ARGLIST [DOCSTRING] STEPS...)
```

Define NAME as a *pact*, a multistep computation intended for private transactions. Identical to *defun* except body must be comprised of *steps*.

```
(defpact payment (payer payer-entity payee
                  payee-entity amount)
  (step-with-rollback payer-entity
    (debit payer amount)
    (credit payer amount))
  (step payee-entity
    (credit payee amount)))
```

defschema

```
(defschema NAME [DOCSTRING] FIELDS...)
```

Define NAME as a *schema*, which specifies a list of FIELDS. Each field is in the form `FIELDNAME[:FIELDTYPE]`.

```
(defschema accounts
  "Schema for accounts table".
  balance:decimal
  amount:decimal
  ccy:string
  data)
```

deftable

```
(deftable NAME[:SCHEMA] [DOCSTRING])
```

Define NAME as a *table*, used in database functions. Note the table must still be created with *create-table*.

let

```
(let (BINDPAIR [BINDPAIR [...]]) BODY)
```

Bind variables in BINDPAIRs to be in scope over BODY. Variables within BINDPAIRs cannot refer to previously-declared variables in the same let binding; for this use *let**.

```
(let ((x 2)
      (y 5))
  (* x y))
> 10
```

let*

```
(let\* (BINDPAIR [BINDPAIR [...]]) BODY)
```

Bind variables in BINDPAIRs to be in scope over BODY. Variables can reference previously declared BINDPAIRS in the same let. `let\*` is expanded at compile-time to nested `let` calls for each BINDPAIR; thus `let` is preferred where possible.

```
(let* ((x 2)
       (y (* x 10)))
  (+ x y))
> 22
```

step

```
(step ENTITY EXPR)
```

Define a step within a *pact*, which can only be executed by nodes representing ENTITY, in order of execution specified in containing *defpact*.

step-with-rollback

```
(step-with-rollback ENTITY EXPR ROLLBACK-EXPR)
```

Define a step within a *pact*, which can only be executed by nodes representing ENTITY, in order of execution specified in containing *defpact*. If any subsequent steps fail, ROLLBACK-EXPR will be executed.

use

```
(use MODULE)
(use MODULE HASH)
```

Import an existing MODULE into namespace. Can only be issued at top-level, or within a module declaration. MODULE can be a string, symbol or bare atom. With HASH, validate that module hash matches HASH, failing if not. Use *describe-module* to query for the hash of a loaded module on the chain.

```
(use accounts)
(transfer "123" "456" 5 (time "2016-07-22T11:26:35Z"))
"Write succeeded"
```

module

```
(module NAME KEYSET [DOCSTRING] DEFS...)
```

Define and install module NAME, guarded by keyset KEYSET, with optional DOCSTRING. DEFS must be *defun* or *defpact* expressions only.

```
(module accounts 'accounts-admin
  "Module for interacting with accounts"

  (defun create-account (id bal)
   "Create account ID with initial balance BAL"
   (insert accounts id { "balance": bal }))

  (defun transfer (from to amount)
   "Transfer AMOUNT from FROM to TO"
   (with-read accounts from { "balance": fbal }
    (enforce (<= amount fbal) "Insufficient funds")
     (with-read accounts to { "balance": tbal }
      (update accounts from { "balance": (- fbal amount) })
      (update accounts to { "balance": (+ tbal amount) }))))
)
```

Expressions

Expressions may be *literals*, atoms, s-expressions, or references.

Atoms

Atoms are non-reserved barewords starting with a letter or allowed symbol, and containing letters, digits and allowed symbols. Allowed symbols are `%#+-_&$@<>=?*!|/`. Atoms must resolve to a variable bound by a *defun*, *defpact*, *binding* form, or to symbols imported into the namespace with *use*.

S-expressions

S-expressions are formed with parentheses, with the first atom determining if the expression is a *special form* or a function application, in which case the first atom must refer to a definition.

Partial application

An application with less than the required arguments is in some contexts a valid *partial application* of the function. However, this is only supported in Pact's *functional-style functions*; anywhere else this will result in a runtime error.

References

References are two atoms joined by a dot `.` to directly resolve to module definitions.

```
pact> accounts.transfer
"(defun accounts.transfer (src,dest,amount,date) \"transfer AMOUNT from
SRC to DEST\")"
pact> transfer
Eval failure:
transfer<EOF>: Cannot resolve transfer
pact> (use 'accounts)
"Using \"accounts\""
pact> transfer
"(defun accounts.transfer (src,dest,amount,date) \"transfer AMOUNT from
SRC to DEST\")"
```

References are preferred to `use` for transactions, as references resolve faster. However in module definition, `use` is preferred for legibility.

CHAPTER 5

Built-in Functions

General

at

idx `integer` *list* `[<l>]` → `<a>`

idx `string` *object* `object:<{o}>` → `<a>`

Index LIST at IDX, or get value with key IDX from OBJECT.

```
pact> (at 1 [1 2 3])
2
pact> (at "bar" { "foo": 1, "bar": 2 })
2
```

bind

src `object:<{row}>` *binding* `binding:<{row}>` *body* `*` → `<a>`

Special form evaluates SRC to an object which is bound to with BINDINGS to run BODY.

```
pact> (bind { "a": 1, "b": 2 } { "a" := a-value } a-value)
1
```

compose

x `(x:<a> -> <b>)` *y* `(x:<b> -> <c>)` *value* `<a>` → `<c>`

Compose X and Y, such that X operates on VALUE, and Y on the results of X.

```
pact> (filter (compose (length) (< 2)) ["my" "dog" "has" "fleas"])
["dog" "has" "fleas"]
```

drop

count `integer` *list* `<a[[<l>],string]>` → `<a[[<l>],string]>`

Drop COUNT values from LIST (or string). If negative, drop from end.

```
pact> (drop 2 "vwxyz")
"xyz"
pact> (drop (- 2) [1 2 3 4 5])
[1 2 3]
```

enforce

test `bool` *msg* `string` → `bool`

Fail transaction with MSG if TEST fails, or returns true.

```
pact> (enforce (!= (+ 2 2) 4) "Chaos reigns")
<interactive>:1:0:(enforce (!= (+ 2 2) 4) "Chaos...: Failure: Tx Failed: Chaos reigns
```

filter

app `(x:<a> -> bool)` *list* `[<a>]` → `[<a>]`

Filter LIST by applying APP to each element to get a boolean determining inclusion.

```
pact> (filter (compose (length) (< 2)) ["my" "dog" "has" "fleas"])
["dog" "has" "fleas"]
```

fold

app `(x:<b> y:<a> -> <a>)` *init* `<a>` *list* `[<b>]` → `<a>`

Iteratively reduce LIST by applying APP to last result and element, starting with INIT.

```
pact> (fold (+) 0 [100 10 5])
115
```

format

template `string` *vars* `*` → `string`

Interpolate VARS into TEMPLATE using {}.

```
pact> (format "My {} has {}" "dog" "fleas")
"My dog has fleas"
```

if

cond `bool` *then* `<a>` *else* `<a>` → `<a>`

Test COND, if true evaluate THEN, otherwise evaluate ELSE.

```
pact> (if (= (+ 2 2) 4) "Sanity prevails" "Chaos reigns")
"Sanity prevails"
```

length

x `<a[[<l>],string,object:<{o}>]>` → `integer`

Compute length of X, which can be a list, a string, or an object.

```
pact> (length [1 2 3])
3
pact> (length "abcdefgh")
8
pact> (length { "a": 1, "b": 2 })
2
```

list

elems `*` → `list`

Create list from ELEMS. Deprecated in Pact 2.1.1 with literal list support.

```
pact> (list 1 2 3)
[1 2 3]
```

list-modules

→ `[string]`

List modules available for loading.

map

app `(x:<b> -> <a>)` *list* `[<b>]` → `[<a>]`

Apply elements in LIST as last arg to APP, returning list of results.

```
pact> (map (+ 1) [1 2 3])
[2 3 4]
```

pact-txid

→ `integer`

Return reference tx id for pact execution.

pact-version

→ `string`

Obtain current pact build version.

```
pact> (pact-version)
"2.2.2"
```

read-decimal

key `string` → `decimal`

Parse KEY string or number value from top level of message data body as decimal.

```
(defun exec ()
   (transfer (read-msg "from") (read-msg "to") (read-decimal "amount")))
```

read-integer

key `string` → `integer`

Parse KEY string or number value from top level of message data body as integer.

```
(read-integer "age")
```

read-msg

→ `<a>`

key `string` → `<a>`

Read KEY from top level of message data body, or data body itself if not provided. Coerces value to pact type: String -> string, Number -> integer, Boolean -> bool, List -> value, Object -> value. NB value types are not introspectable in pact.

```
(defun exec ()
   (transfer (read-msg "from") (read-msg "to") (read-decimal "amount")))
```

remove

key `string` *object* `object:<{o}>` → `object:<{o}>`

Remove entry for KEY from OBJECT.

```
pact> (remove "bar" { "foo": 1, "bar": 2 })
{"foo": 1}
```

resume

binding `binding:<{y}>` *body* `*` → `<a>`

Special form binds to a yielded object value from the prior step execution in a pact.

take

count `integer` *list* `<a[[<l>],string]>` → `<a[[<l>],string]>`

Take COUNT values from LIST (or string). If negative, take from end.

```
pact> (take 2 "abcd")
"ab"
pact> (take (- 3) [1 2 3 4 5])
[3 4 5]
```

typeof

x `<a>` → `string`

Returns type of X as string.

```
pact> (typeof "hello")
"string"
```

yield

OBJECT `object:<{y}>` → `object:<{y}>`

Yield OBJECT for use with 'resume' in following pact step. The object is similar to database row objects, in that only the top level can be binded to in 'resume'; nested objects are converted to opaque JSON values.

```
(yield { "amount": 100.0 })
```

Database

create-table

table `table:<{row}>` → `string`

Create table TABLE.

```
(create-table accounts)
```

describe-keyset

keyset `string` → `value`

Get metadata for KEYSET

describe-module

module `string` → `value`

Get metadata for MODULE. Returns a JSON object with 'name', 'hash' and 'code' fields.

describe-table

table `string` → `value`

Get metadata for TABLE

insert

table `table:<{row}>` *key* `string` *object* `object:<{row}>` → `string`

Write entry in TABLE for KEY of OBJECT column data, failing if data already exists for KEY.

```
(insert 'accounts { "balance": 0.0, "note": "Created account." })
```

keys

table `table:<{row}>` → `[string]`

Return all keys in TABLE.

```
(keys 'accounts)
```

read

table `table:<{row}>` *key* `string` → `object:<{row}>`

table `table:<{row}>` *key* `string` *columns* `[string]` → `object:<{row}>`

Read row from TABLE for KEY returning database record object, or just COLUMNS if specified.

```
(read 'accounts id ['balance 'ccy])
```

txids

table `table:<{row}>` *txid* `integer` → `[integer]`

Return all txid values greater than or equal to TXID in TABLE.

```
(txids 'accounts 123849535)
```

txlog

table `table:<{row}>` *txid* `integer` → `[value]`

Return all updates to TABLE performed in transaction TXID.

```
(txlog 'accounts 123485945)
```

update

table `table:<{row}>` *key* `string` *object* `object:<{row}>` → `string`

Write entry in TABLE for KEY of OBJECT column data, failing if data does not exist for KEY.

```
(update 'accounts { "balance": (+ bal amount), "change": amount, "note": "credit" })
```

with-default-read

table `table:<{row}>` *key* `string` *defaults* `object:<{row}>` *bindings* `binding:<{row}>` → <a>

Special form to read row from TABLE for KEY and bind columns per BINDINGS over subsequent body statements. If row not found, read columns from DEFAULTS, an object with matching key names.

```
(with-default-read 'accounts id { "balance": 0, "ccy": "USD" } { "balance":= bal, "ccy
↪":= ccy }
   (format "Balance for {} is {} {}" id bal ccy))
```

with-read

table `table:<{row}>` *key* `string` *bindings* `binding:<{row}>` → <a>

Special form to read row from TABLE for KEY and bind columns per BINDINGS over subsequent body statements.

```
(with-read 'accounts id { "balance":= bal, "ccy":= ccy }
   (format "Balance for {} is {} {}" id bal ccy))
```

write

table `table:<{row}>` *key* `string` *object* `object:<{row}>` → `string`

Write entry in TABLE for KEY of OBJECT column data.

```
(write 'accounts { "balance": 100.0 })
```

Time

add-time

time `time` *seconds* `decimal` → `time`

time `time` *seconds* `integer` → `time`

Add SECONDS to TIME; SECONDS can be integer or decimal.

```
pact> (add-time (time "2016-07-22T12:00:00Z") 15)
"2016-07-22T12:00:15Z"
```

days

n `decimal` → `decimal`

n `integer` → `decimal`

N days, for use with 'add-time'

```
pact> (add-time (time "2016-07-22T12:00:00Z") (days 1))
"2016-07-23T12:00:00Z"
```

diff-time

time1 `time` *time2* `time` → `decimal`

Compute difference between TIME1 and TIME2 in seconds.

```
pact> (diff-time (parse-time "%T" "16:00:00") (parse-time "%T" "09:30:00"))
23400
```

hours

n `decimal` → `decimal`

n `integer` → `decimal`

N hours, for use with 'add-time'

```
pact> (add-time (time "2016-07-22T12:00:00Z") (hours 1))
"2016-07-22T13:00:00Z"
```

minutes

n `decimal` → `decimal`

n `integer` → `decimal`

N minutes, for use with 'add-time'.

```
pact> (add-time (time "2016-07-22T12:00:00Z") (minutes 1))
"2016-07-22T12:01:00Z"
```

parse-time

format `string` *utcval* `string` → `time`

Construct time from UTCVAL using FORMAT. See strftime docs for format info.

```
pact> (parse-time "%F" "2016-09-12")
"2016-09-12T00:00:00Z"
```

time

utcval `string` → `time`

Construct time from UTCVAL using ISO8601 format (%Y-%m-%dT%H:%M:%SZ).

```
pact> (time "2016-07-22T11:26:35Z")
"2016-07-22T11:26:35Z"
```

Operators

!=

x `<a[integer,string,time,decimal,bool,[<l>],object:<{o}>,keyset]>` *y* `<a[integer,string,time,decimal,bool,[<l>],object:<{o}>,keyset]>` → `bool`

True if X does not equal Y.

```
pact> (!= "hello" "goodbye")
true
```

*

x `<a[integer,decimal]>` *y* `<a[integer,decimal]>` → `<a[integer,decimal]>`

x `<a[integer,decimal]>` *y* `<b[integer,decimal]>` → `decimal`

Multiply X by Y.

```
pact> (* 0.5 10.0)
5
pact> (* 3 5)
15
```

+

x `<a[integer,decimal]>` *y* `<a[integer,decimal]>` → `<a[integer,decimal]>`

x `<a[integer,decimal]>` *y* `<b[integer,decimal]>` → `decimal`

x `<a[string,[<l>],object:<{o}>]>` *y* `<a[string,[<l>],object:<{o}>]>` → `<a[string,[<l>],object:<{o}>]>`

Add numbers, concatenate strings/lists, or merge objects.

```
pact> (+ 1 2)
3
pact> (+ 5.0 0.5)
5.5
pact> (+ "every" "body")
"everybody"
pact> (+ [1 2] [3 4])
[1 2 3 4]
```

```
pact> (+ { "foo": 100 } { "foo": 1, "bar": 2 })
{"bar": 2, "foo": 100}
```

-

x <a[integer,decimal]> *y* <a[integer,decimal]> → <a[integer,decimal]>

x <a[integer,decimal]> *y* <b[integer,decimal]> → decimal

x <a[integer,decimal]> → <a[integer,decimal]>

Negate X, or subtract Y from X.

```
pact> (- 1.0)
-1.0
pact> (- 3 2)
1
```

/

x <a[integer,decimal]> *y* <a[integer,decimal]> → <a[integer,decimal]>

x <a[integer,decimal]> *y* <b[integer,decimal]> → decimal

Divide X by Y.

```
pact> (/ 10.0 2.0)
5
pact> (/ 8 3)
2
```

<

x <a[integer,decimal,string,time]> *y* <a[integer,decimal,string,time]> → bool

True if X < Y.

```
pact> (< 1 3)
true
pact> (< 5.24 2.52)
false
pact> (< "abc" "def")
true
```

<=

x <a[integer,decimal,string,time]> *y* <a[integer,decimal,string,time]> → bool

True if X <= Y.

```
pact> (<= 1 3)
true
pact> (<= 5.24 2.52)
false
```

```
pact> (<= "abc" "def")
true
```

=

x <a[integer,string,time,decimal,bool,[<l>],object:<{o}>,keyset]> *y* <a[integer,string,time,decimal,bool,[<l>],object:<{o}>,keyset]> → bool

True if X equals Y.

```
pact> (= [1 2 3] [1 2 3])
true
pact> (= 'foo "foo")
true
pact> (= { 1: 2 } { 1: 2})
true
```

>

x <a[integer,decimal,string,time]> *y* <a[integer,decimal,string,time]> → bool

True if X > Y.

```
pact> (> 1 3)
false
pact> (> 5.24 2.52)
true
pact> (> "abc" "def")
false
```

>=

x <a[integer,decimal,string,time]> *y* <a[integer,decimal,string,time]> → bool

True if X >= Y.

```
pact> (>= 1 3)
false
pact> (>= 5.24 2.52)
true
pact> (>= "abc" "def")
false
```

^

x <a[integer,decimal]> *y* <a[integer,decimal]> → <a[integer,decimal]>

x <a[integer,decimal]> *y* <b[integer,decimal]> → decimal

Raise X to Y power.

```
pact> (^ 2 3)
8
```

abs

x `decimal` → `decimal`

x `integer` → `integer`

Absolute value of X.

```
pact> (abs (- 10 23))
13
```

and

x `bool` *y* `bool` → `bool`

Boolean logic.

```
pact> (and true false)
false
```

ceiling

x `decimal` *prec* `integer` → `decimal`

x `decimal` → `integer`

Rounds up value of decimal X as integer, or to PREC precision as decimal.

```
pact> (ceiling 3.5)
4
pact> (ceiling 100.15234 2)
100.16
```

exp

x `<a[integer,decimal]>` → `<a[integer,decimal]>`

Exp of X

```
pact> (round (exp 3) 6)
20.085537
```

floor

x `decimal` *prec* `integer` → `decimal`

x `decimal` → `integer`

Rounds down value of decimal X as integer, or to PREC precision as decimal.

```
pact> (floor 3.5)
3
pact> (floor 100.15234 2)
100.15
```

ln

x <a[integer,decimal]> → <a[integer,decimal]>

Natural log of X.

```
pact> (round (ln 60) 6)
4.094345
```

log

x <a[integer,decimal]> *y* <a[integer,decimal]> → <a[integer,decimal]>

x <a[integer,decimal]> *y* <b[integer,decimal]> → decimal

Log of Y base X.

```
pact> (log 2 256)
8
```

mod

x integer *y* integer → integer

X modulo Y.

```
pact> (mod 13 8)
5
```

not

x bool → bool

Boolean logic.

```
pact> (not (> 1 2))
true
```

or

x bool *y* bool → bool

Boolean logic.

```
pact> (or true false)
true
```

round

x decimal *prec* integer → decimal

x decimal → integer

Performs Banker's rounding value of decimal X as integer, or to PREC precision as decimal.

```
pact> (round 3.5)
4
pact> (round 100.15234 2)
100.15
```

sqrt

x `<a[integer,decimal]>` → `<a[integer,decimal]>`

Square root of X.

```
pact> (sqrt 25)
5
```

Keysets

define-keyset

name `string` *keyset* `string` → `string`

Define keyset as NAME with KEYSET. If keyset NAME already exists, keyset will be enforced before updating to new value.

```
(define-keyset 'admin-keyset (read-keyset "keyset"))
```

enforce-keyset

keyset-or-name `<k[string,keyset]>` → `bool`

Special form to enforce KEYSET-OR-NAME against message keys before running BODY. KEYSET-OR-NAME can be a symbol of a keyset name or a keyset object.

```
(with-keyset 'admin-keyset ...)
(with-keyset (read-keyset "keyset") ...)
```

keys-2

count `integer` *matched* `integer` → `bool`

Keyset predicate function to match at least 2 keys in keyset.

```
pact> (keys-2 3 1)
false
```

keys-all

count `integer` *matched* `integer` → `bool`

Keyset predicate function to match all keys in keyset.

```
pact> (keys-all 3 3)
true
```

keys-any

count `integer` *matched* `integer` → `bool`

Keyset predicate function to match any (at least 1) key in keyset.

```
pact> (keys-any 10 1)
true
```

read-keyset

key `string` → `keyset`

Read KEY from message data body as keyset ({ "keys": KEYLIST, "pred": PREDFUN }). PREDFUN should resolve to a keys predicate.

```
(read-keyset "admin-keyset")
```

REPL-only functions

The following functions are loaded magically in the interactive REPL, or in script files with a `.repl` extension. They are not available for blockchain-based execution.

begin-tx

→ `string`

name `string` → `string`

Begin transaction with optional NAME.

```
(begin-tx "load module")
```

bench

exprs `*` → `string`

Benchmark execution of EXPRS.

```
(bench (+ 1 2))
```

commit-tx

→ `string`

Commit transaction.

```
(commit-tx)
```

env-data

json `<a[integer,string,time,decimal,bool,[<l>],object:<{o}>,keyset,value]>` → `string`

Set transaction JSON data, either as encoded string, or as pact types coerced to JSON.

```
pact> (env-data { "keyset": { "keys": ["my-key" "admin-key"], "pred": "keys-any" } })
"Setting transaction data"
```

env-entity

entity `string` → `string`

Set environment confidential ENTITY id. Also clears last expression's yield value.

```
(env-entity "my-org")
```

env-keys

keys `[string]` → `string`

Set transaction signature KEYS.

```
pact> (env-keys ["my-key" "admin-key"])
"Setting transaction keys"
```

env-step

→ `string`

step-idx `integer` → `string`

step-idx `integer` *rollback* `bool` → `string`

step-idx `integer` *rollback* `bool` *resume* `object:<{y}>` → `string`

Modify pact step state. With no arguments, unset step. With STEP-IDX, set step index to execute. ROLLBACK instructs to execute rollback expression, if any. RESUME sets the value of a previous YIELD step.Also clears last expression's yield value.

```
(env-step 1)
(env-step 0 true)
```

expect

doc `string` *expected* <a> *actual* <a> → `string`

Evaluate ACTUAL and verify that it equals EXPECTED.

```
pact> (expect "Sanity prevails." 4 (+ 2 2))
"Expect: success: Sanity prevails."
```

expect-failure

doc `string` *exp* <a> → `string`

Evaluate EXP and succeed only if it throws an error.

```
pact> (expect-failure "Enforce fails on false" (enforce false "Expected error"))
"Expect failure: success: Enforce fails on false"
```

json

exp <a> → `value`

Encode pact expression EXP as a JSON value. This is only needed for tests, as Pact values are automatically represented as JSON in API output.

```
pact> (json [{ "name": "joe", "age": 10 } {"name": "mary", "age": 25 }])
[{"age":10,"name":"joe"},{"age":25,"name":"mary"}]
```

load

file `string` → `string`

file `string` *reset* `bool` → `string`

Load and evaluate FILE, resetting repl state beforehand if optional NO-RESET is true.

```
(load "accounts.repl")
```

print

value <a> → `string`

Print a string, mainly to format newlines correctly

rollback-tx

→ `string`

Rollback transaction.

```
(rollback-tx)
```

sig-keyset

→ `keyset`

Convenience to build a keyset from keys present in message signatures, using 'keys-all' as the predicate.

typecheck

module `string` → `string`

module `string` *debug* `bool` → `string`

Typecheck MODULE, optionally enabling DEBUG output.

yielded

expect-yield `bool` → `<a>`

When EXPECT-YIELD is true, return result of yield from previous evaluation, failing if not set. When EXPECT-YIELD is false, fail if the previous evaluation produced a yield.