

Gear technical

Abstract

This paper covers technical aspects of Gear, a new Polkadot/Kusama parachain and smart-contract engine for networks with untrusted code.

Gear provides an engine for Polkadot/Kusama parachains and standalone bridged blockchains. Gear allows to run WebAssembly programs (smart-contracts) compiled from many popular languages, such as C/C++, Rust and more.

Gear smart-contract architecture utilizes advantages of an actor communication model, enables persistent memory for immutable programs and ensures very minimal, intuitive and sufficient api surface for blockchain context.

1. General outline

A short description of Substrate blockchain framework is given in section (2).

An overview of Polkadot Network and Gear's role in it are described in section (3).

The distinctive characteristics and components of the Gear's network state are covered in section (4), details about how the Gear's network state evolves are provided in section (5).

Balance transfers, Gas economy and DoS protection are covered in section (6).

For inter-process (or cross-contract) communications, actor model is used. How it is organized inside the Gear state and what it brings to the table of decentralized computations is covered in section (7).

Typical scenario of how Gear processes inputs from user interactions with program are discussed in section (8).

A WebAssembly virtual machine used in Gear network and notable features introduced for VM implementation are covered in section (9).

2. Substrate framework

Substrate blockchain framework is an important component of Polkadot Network. It allows every team creating a new blockchain not to waste efforts for implementation of the networking and consensus code from scratch.

Substrate covers both - replication (networking layer) and fault-tolerance (consensus mechanism). Technical description of those layers is beyond the scope of this paper. Refer to [Substrate Documentation](#) for more details.

Gear uses the Substrate framework under the hood. It covers the most desired requirements for enterprise-ready decentralized projects - fault tolerance, replication, tokenization, immutability, data security and production ready cross-platform persistent database.

Gear itself is implemented as a custom Substrate runtime. It also introduces advanced native extensions (via host functions) for performance.

Using Substrate allows to quickly connect Gear instances as parachain/parathread into the Polkadot/Kusama network.

3. Polkadot Network

Polkadot is a next-generation blockchain protocol intended to unite multiple purpose-built blockchains, allowing them to operate seamlessly together at scale.

There are several components in the Polkadot architecture, namely: - Relay Chain
- Parachains - Bridges

Relay Chain

Relay Chain is the heart of Polkadot, responsible for the network's security, consensus and cross-chain interoperability.

Parachains

Parachains are sovereign blockchains that can have their own tokens and optimize their functionality for specific use cases. Parachains must be connected to the Relay Chain to ensure interoperability with other networks. For this, parachains can pay as they go or lease a slot for continuous connectivity.

Bridges

A blockchain bridge is a special connection that allows Polkadot ecosystem to connect to and communicate with external networks like Ethereum, Bitcoin and others. Such connection allows transfer of tokens or arbitrary data from one blockchain to another.

Polkadot communication model and Gear role

The critical aspect of Polkadot network is its ability to route arbitrary messages between chains. Using this messages is as simple as it can be: negotiate the channel between two parachains and send asynchronous messages through it.

Polkadot Relay Chain and Gear ultimately speak the same language (asynchronous messages). Projects building on Gear can seamlessly integrate their solutions into the whole Polkadot/Kusama ecosystem.

Asynchronous messaging architecture allows Gear to be an effective and easy-to-use parachain of Polkadot network:

1. Users deploy programs to Gear network.
2. Individual channels are established to popular parachains or bridges (there can be many and competing).
3. The whole Gear parachain communicates through them.

Such architecture allows driving the transition of network between states and fits nicely to the whole network.

4. State

As any blockchain system, Gear maintains distributed state. Runtime code compiled to WebAssembly becomes part of the blockchain's storage state.

Gear ensures one of the defining features - forkless runtime upgrades. The state is also guaranteed to be finalized if finality gadget is used.

Storage state components

- **Programs and memory** (includes program's code and private memory)
- **Message queue** (global message queue of the network)
- **Accounts** (network accounts and their balances)

Programs

Programs are first-class citizens in the Gear instance state.

Program code is stored as an immutable Wasm blob. Each program has a fixed amount of memory which persists between message-handling (so-called static area).

Programs can allocate more memory from the memory pool provided by the Gear instance. A particular program can read and write only within exclusively allocated to it memory.

Memory

Gear instance holds individual memory space per program and guarantees it's persistence. A program can read and write only within its own memory space and have no access to the memory space of other programs. Individual memory space is reserved for a program during its initialization and does not require additional fee (included in the program initialization fee).

A program can allocate the required amount of memory in blocks of 64KB. Each memory block allocation requires gas fee. Each page (64KB) is stored separately on the distributed database backend, but at the run time, Gear node constructs continuous runtime memory and allows programs to run on it without reloads.

GEAR instance			
Reserved private memory		Reserved private memory	
</PROGRAM A> (1 allocation)		</PROGRAM B> (2 allocation)	
PAGE 1 (Allocated)	PAGE 2	PAGE 1 (Allocated)	PAGE 2 (Allocated)
PAGE 3	PAGE 4	PAGE 3	PAGE 4
-	-	-	-
PAGE N-3	PAGE N-2	PAGE N-3	PAGE N-2
PAGE N-1	PAGE N	PAGE N-1	PAGE N
Reserved private memory		Reserved private memory	
</PROGRAM C> (0 allocation)			
PAGE 1	PAGE 2		
PAGE 3	PAGE 4		
-	-		
PAGE N-3	PAGE N-2		
PAGE N-1	PAGE N		
Reserved private memory		Reserved private memory	

Message queue

Gear instance holds global message queue. Using Gear node, users can send transactions with one or several messages to a particular program(s). This fills up the message queue. During block construction, messages are dequeued and routed to the particular program.

Accounts

For a public network, protection against DOS attacks always requires economic incentives. Thus, Gear network tracks balances of programs and users.

In general, a particular Gear network instance can be defined as both permissioned and permissionless, public blockchain. In the permissioned scenario, no balance module is required.

5. State transition

Each system follows the rules according to which the state of the system evolves.

As network processes new input data, state is advanced according to state transition rules. This input data is packed in atomic pieces of information called transactions. Gear nodes maintains and synchronizes transaction pool which contains all that new transactions. When any node (validator or not) receives a transaction, the node propagates the transaction to all connected nodes. For advanced reading how transaction pool operates, refer to [Substrate Documentation](#).

When a Gear validator node comes to produce a new block, some (or all) transactions from the pool are merged into a block and network undergoes a state transition via this block. Transactions that were not taken in the last block remain in the pool until the next block producing.

Gear supports the following types of transactions:

1. **Create a program** (user uploads new programs - smart-contracts)
2. **Send a message** (program fills the message queue)
3. **Dequeue messages** (validators (block producers) dequeue multiple messages, running associated programs)
4. **Balance transfers** (Gear engine performs user-program-validator balance transfers)

Message processing is performed in the reserved space of the block construction/import time. It is guaranteed that message processing will be executed in every block, and at least at some particular rate determined by current instance settings.

Create a program

Designated authorities (or any user for public implementation) of Gear network can propose a new program saved to the state. For public networks, a balance associated with a program is also provided. This new balance then constitutes the initial balance (Existential Deposit).

Send a message

End-users interact with programs and as a result, send messages to Gear network. Messages sent to the Gear network fill up the global message queue. This queue can be viewed as a runtime-driven transaction queue but with the guarantee that any message accepted into it will eventually be processed. Putting a message in the queue is not free and therefore a message is guaranteed to be dispatched.

Dequeue messages

Validators can choose which messages to dequeue when it's their turn to produce the next block. It eliminates the need of each particular validator to maintain the full memory state. Dequeuing occurs only at the end of each block. During

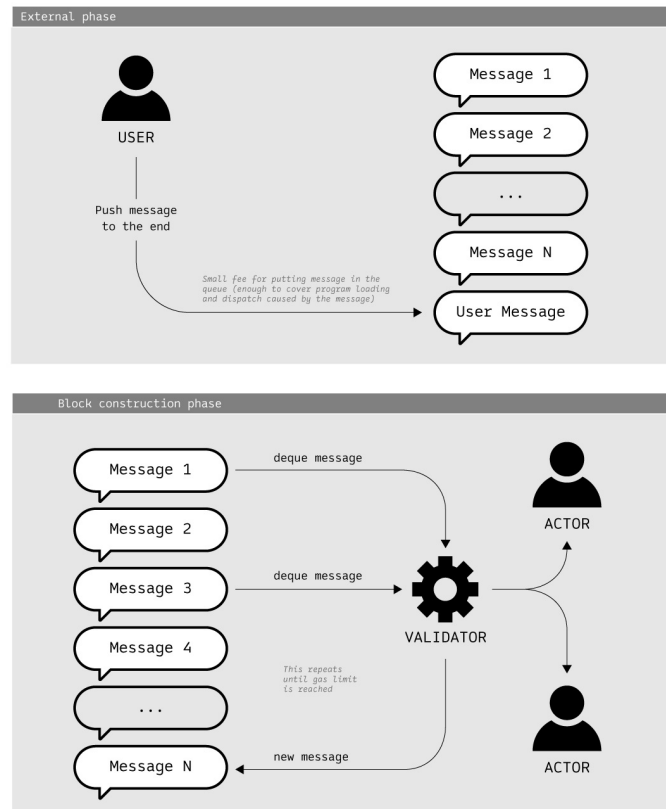
dequeuing, new messages can be generated. They can also be processed in this phase, but also can stay in the queue for the next block (and another validator).

Balance transfers

Regular balance transfers are performed inside Substrate Balances module. Refer to the next chapter for more details.

Messages, blocks and events lifecycle

The picture below illustrates eternal lifecycle of Gear machinery. As actor model for communications dictates, nothing is shared, there are only messages. Messages with destination “system” end up in the event log to be inspected in the user space.



6. Balance transfers and gas economy

Regular balance transfer is performed inside Substrate Balances module. Balance is transferred between user, program and validator accounts.

In addition to regular balance transfer Gear network defines gas balance transfer that is used to reward validator nodes for their work and allows network to be protected from DoS attacks.

Gear node charges gas fee during message processing. The message processing algorithm is described below in details.

All interactions inside Gear network are done via messaging. Messages in Gear have common interface with the following parameters:

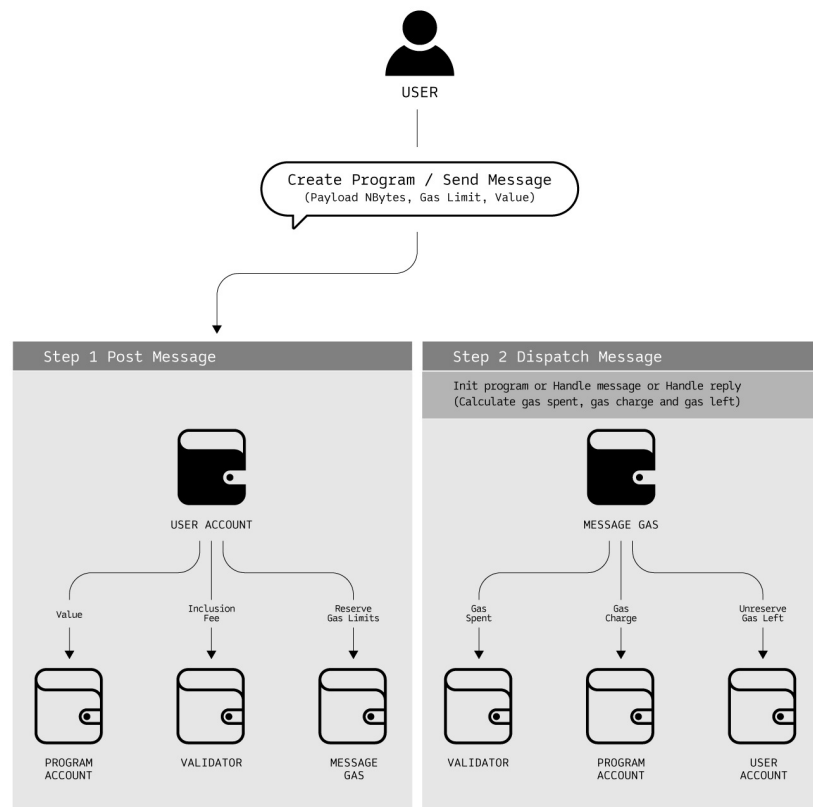
- source account,
- target account,
- payload,
- gas_limit
- value

There are five types of messages used in Gear network:

1. A special message from user to upload a new program to the network.
Payload must contain Wasm file of the program itself. Target account must not be specified - it will be created as a part of processing message post.
2. From user to program
3. From program to program
4. From program to user
5. From user to user

The last parameter of send message function is a value to be transferred to target account. In the special message of the initial program upload, value will be transferred to a balance of the newly created account for the program.

Message processing consists of two steps:



Step one

Gear network tries to post a message into the queue that aims to verify the source account has enough balance to cover sending of *value* and *gas_limit* and paying of small processing fee that is linearly depends on payload size (this is the standard inclusion fee for Substrate framework, refer to [Substrate Documentation](#) for details).

After validation, block producer of Gear network posts the message into the block, transfers *value* to the target account, transfers small processing fee to the validator account and reserves fee equal to *gas_limit* on source account.

Step two

A program message is dispatched by the network in the following way:

When uploading a program user specifies *gas_limit* and optionally *value* to be transferred to program account. *gas_limit* serves as a maximum amount of gas to be spent on program initialization.

When a program is being initialized by Gear node it consumes gas for both - per memory page allocation and per cpu instructions. It increments the internal counter - *gas_spent*.

Gear node checks on each increment of *gas_spent* that its value is lower than *gas_limit* specified in initialization message and if it is more, then it stops program execution. This way *gas_limit* serves as a safeguard for user balance so no program will consume more than user expects.

Optionally program can try to reserve additional gas for its own balance for the sake of sending messages to other programs in the future or during initialization. It can be done by using special instruction *gas_charge*. When specified, a Gear node automatically checks that *gas_spent* plus *gas_charge* is below *gas_limit* specified in message. Another way to increase balance of program is to specify explicitly transfer value to its balance using last parameter of initialization message.

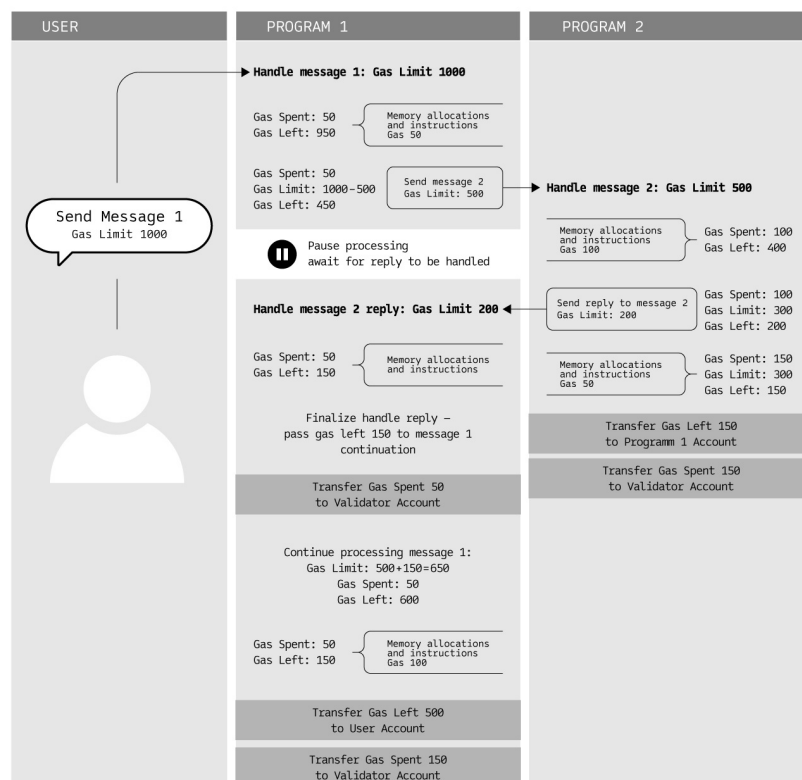
After program has been initialized, *gas_spent* is charged against user account towards validator's account, and *gas_charge* is charged against user account to program account.

The difference between *gas_limit* and *gas_spent* plus *gas_charge* is *gas_left* and its value is unreserved on source account.

Gas fee is linear - 64000 gas per allocated memory page of size 64KB and 1000 gas per instrumented Wasm instruction.

For standard messages where the target is a program, all of the above gas consumption rules apply as well as additional memory rent fee is charged via incrementing *gas_spent* value. This memory rent fee is similar to memory allocation fee but the price is lower than the one for initial allocation - 1000 gas per already allocated page. Memory rent is charged because of node has to load/save program memory from/to network state.

The picture below shows more detailed example of balance transfers:



7. Actor model for communications

For inter-process communications, Gear uses Actor model approach. The actor model has recently become increasingly popular and finds its way into many new programming languages, often as first-class language concept. The principles of Actor model is that programs never share any state and just exchange messages between each other.

While in an ordinary actor model, there is no guarantee on message ordering, Gear makes some extra guarantees. Gear guarantees that order of messages between two particular programs is preserved.

Using Actor model approach gives way to implement Actor-based concurrency inside programs (smart-contracts) logic. This can utilize various language constructs for asynchronous programming (for example, Futures and `async-await` in Rust).

8. Typical scenario

Let's take a look how Gear machinery works when running imaginary program.

Gear allows any general-purpose language program compiled to WebAssembly to run, for example this `capacitor.rs`:

```
static mut CHARGE: u32 = 0;

static mut LIMIT: u32 = 0;

static mut DISCHARGE_HISTORY: Vec<u32> = Vec::new();

#[no_mangle]
pub unsafe extern "C" fn handle() {
    let new_msg = String::from_utf8(msg::load()).expect("Invalid
        message: should be utf-8");

    let to_add = u32::from_str(&new_msg).expect("Invalid number");

    CHARGE += to_add;

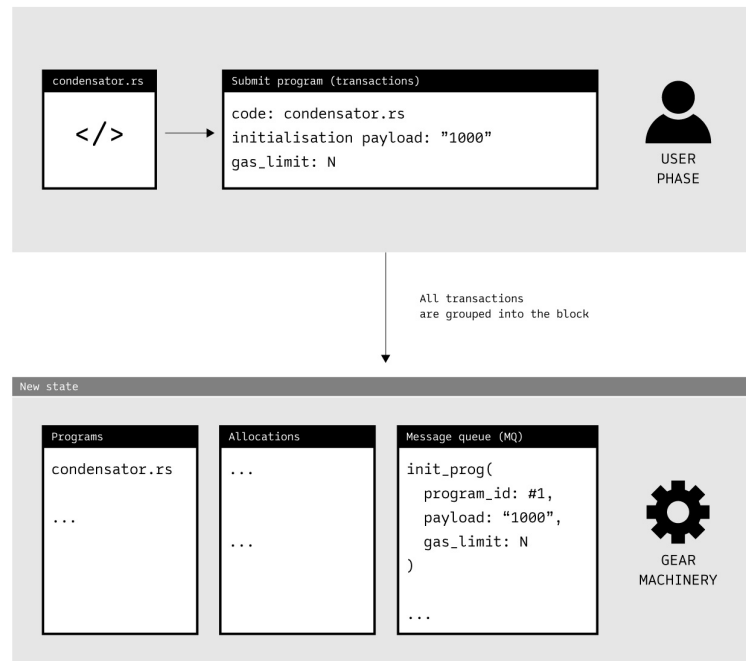
    if CHARGE >= LIMIT {
        DISCHARGE_HISTORY.push(CHARGE);
        msg::send(0.into(), format!("Discharged: {}",
            CHARGE).as_bytes(), 1000000000);
        CHARGE = 0;
    }
}
```

For full example, refer to [our test crate](#).

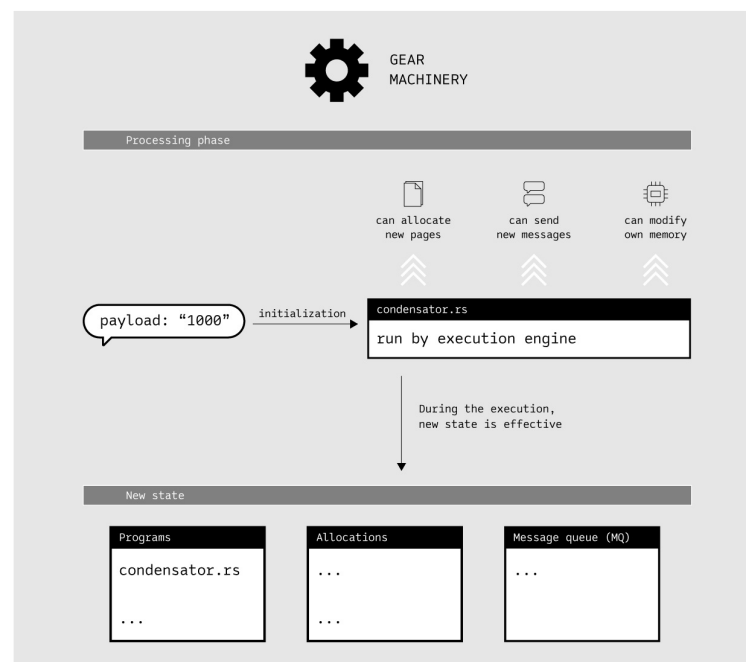
This is a simple program that “charges” with incoming messages and “discharges” when total amount of “charge” exceeds some limit provided in initialization.

Let's take a look on series of diagrams illustrating how user creates such a program and then interacts with it:

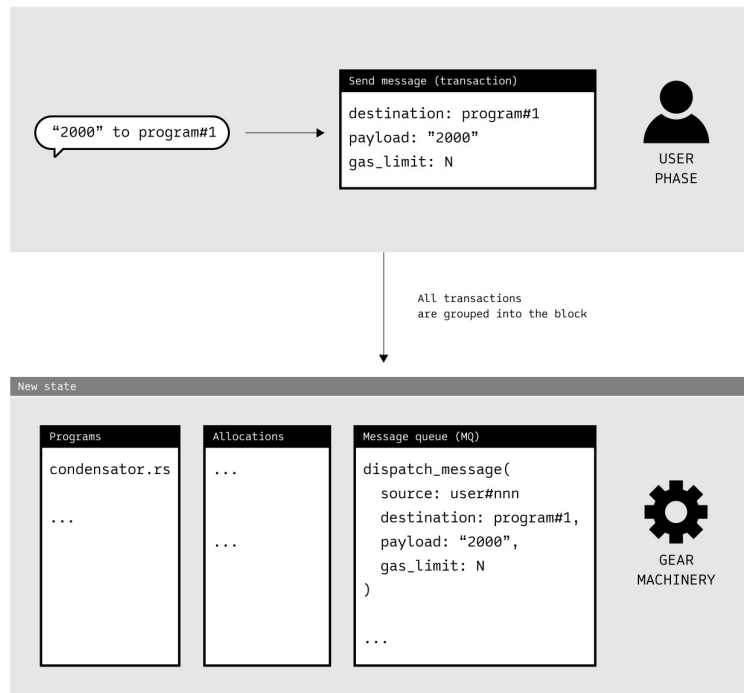
1. This is how the program is created - user just sends a transaction with program and initialization arguments:



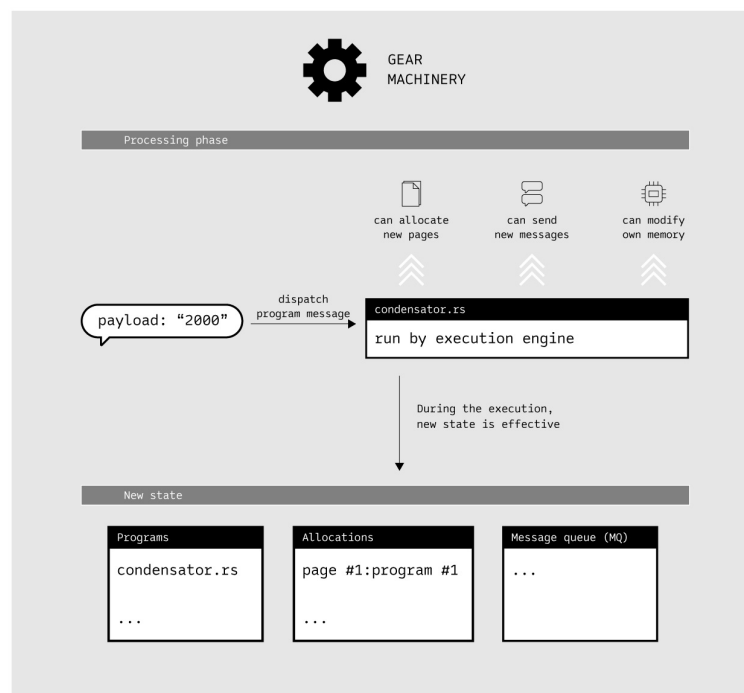
2. Gear then processes this new input:



3. Once created, program can receive messages. For example, user can send “charge” of 2000 to it:



4. Gear then process this new input:



9. Virtual machine (WebAssembly)

Gear uses WebAssembly (or Wasm) under the hood. Any Gear program is in WebAssembly format.

WebAssembly is a code format for deploying programs. In Gear context, any smart-contract is a WebAssembly program.

WebAssembly has the following advantages:

- Native speed. As it translates to actual hardware instructions.
- Portable. It can run on any actual hardware.
- Safe. Properly validated WebAssembly program cannot leave sandbox (guaranteed by specification).

WebAssembly is a global industrial technology, remarkable for many reasons:

- It has been designed and implemented in collaboration between all major competitors in its space.
- It has been designed and released along with a complete mathematical, machine-verified formalisation.

10. Applicability and use cases

Micro/nanoservices

Years ago, software development moved from monolithic to microservice architecture. Addressing complexities of previous approach related to tightly coupled, interconnected code. In recent years, nanoservices have become mainstream to address known microservice complexity.

Any general-purpose language nanoservice function compiled to Wasm can be uploaded as a program to Gear. Gear will execute the code to process a certain task within necessary timeframe. Gear provides automatic seamless scalability according to the number of tasks necessary to process. You only pay for the resources your function consumes.

In interaction with other nanoservices in Gear, you get an applicable architecture out of the box. Just focus on the pieces of code that matter to you, and Gear handles the rest.