

## Atomchain Payment Transactions: Alpha and Omega Scheme

**Author:** Okpara Okechukwu D. **Email:** okpara.net@gmail.com

**Website:** www.okpara.net **Date:** 05-05-2022

### 1. Introduction

Atomchain can be considered as a distributed, verifiable append-only timestamped database (or data store) structure. This structure contains a robust and auditable registry of all transactions. In the Atom Network's Mainnet (called The Universe), the database is mostly secured and managed by perfect nodes - peers with "atomRepute" of 100%. These peers are usually granted central atomic roles.

Also, atomchain (or atomsphere) can be considered as a distributed database that is organized as a multi-linked list of encapsulated (or ordered) atoms, where the inner (or committed) atoms starting from the atomcore are immutable.

Atomchain has both the Turing-complete capability of EVM/Ethereum-like blockchains and the Script/UTXO capability of Bitcoin-like blockchains. Note that in the latter case, only one cryptocurrency is supported on the blockchain at a time, but with Atomchain multiple Bitcoin-like cryptocurrencies can be defined using a confirmed omega-operator atom, such that these multiple coins are pegged to atomcoins/OKE as their unit of exchange. In other words, since both alpha and omega atoms consume energy in units of atomcoins/OKE, Bitcoin and alternative coins (altcoins) can coexist on Atomchain. The only issue is that these coins' consensus mechanisms (PoW, PoS, PoA, etc) has to be adjusted to the atomchain's elevatedModes algorithm and P2P network implementations.

Atomcoin is the protocol token of the atomchain's cryptoverse. Atomcoin is supposed to have three functions: a store of value, a unit of account, and a medium of exchange. Stability is the main key to all these functions. Store of value is the most salient; if people store their wealth in an asset that constantly fluctuates in value, their wealth will fluctuate accordingly. A volatile asset is also a poor unit of account, because it is inconvenient to denominate prices in something which constantly changes in value. Every time the value of the unit of account changes, all prices must be adjusted accordingly. Finally, and most crucially, a currency needs to be stable to function as a medium of exchange; this allows people to be fairly and predictably compensated for goods and services without changes in value during the payment process.

### 2. Atomchain Payment Transactions

Atomchain Payment Transactions associated with Atom Wallets can be done through **alpha( $\alpha$ )** or **omega( $\Omega$ )** scheme. The alpha scheme can be applied to payment transactions, but the omega schemes can be applied to both payment and nonpayment transactions. In an alpha scheme, a payment transaction usually includes the payee's identity ( $\alpha$  address) to specify the designated recipient of a payment. Alpha-based payment is a Pay-to-Shell(P2S) or a Pay-to-Public-Key-Hash (P2PKH) transaction, referred to as Pay-to-World-Hash-Object (P2WHO) —and it includes the hash of the public key (or World) of payee and the amount (an  $\alpha$  Object) to be paid to this payee in a transaction format according to **Atomchain Objective-O** Model, which aims to use the advantages associated with  $\alpha$  scheme to solve the intrinsic problems of  $\Omega$  scheme, as well as, using the advantages of  $\Omega$  scheme to handle intrinsic issues of  $\alpha$  scheme.

**Note:** for better understanding by those familiar with blockchain, refer to a 'private key' as "home," and a 'public key' as "world". A world is a single 160-bit identifier often used with  $\Omega$  addresses. A Shell is a deployed-script  $\alpha$  address.

### 3. Atom Wallets:

Digital atom wallets via home-world key pairs can facilitate many tasks associated with “**transaction balances**”; such as storing keys, setting transaction energy fees, providing **return change** addresses, and handling transaction balances, including aggregating them to show available, pending, and total balances.

**Note:** If a user spends, for instance, 0.5 atomcoin using a transaction balance of 1 atomcoin of an only **α address** atom wallet, they must deliberately self-address (or send to themselves) the remaining 0.5 atomcoin to that address as a return change. Failure to send the  $(1 - 0.5 = 0.5)$  atomcoin change will result in them losing their change to any atom creator who mines their transaction.

On the other hand, a  $\Omega$ -address is a “transaction-event state”. The first states of  $\Omega$  addresses are defined in the Atomcore. Unlike  $\alpha$  address, transaction balances are not stored directly on  $\Omega$  address. Only the root node hashes (consisting of transaction root, state root and receipt root) of the transaction trie, state trie, and receipts trie (respectively) are stored directly in atomchain using  $\Omega$  addresses. Transaction trie contains transaction data which is permanent or immutable. Storage trie contains all quark code data; it can also contain a “transaction balance” of  $\Omega$  address. The transaction balance of  $\Omega$  address stored in the state trie can be altered whenever transactions against that  $\Omega$  address occur. The state trie’s root node ( a hash of the entire state trie at a given point in time) is used as a secure and unique identifier for the state trie; the state trie’s root node is also cryptographically dependent on all internal state trie data. A 256-bit hash of the storage trie’s root node is stored as the storage root value in the global state trie.

Each atom has its own transaction trie. An atom contains many transactions assembled by the atom creator. The path to a specific transaction in the transaction trie, is through (the Recursive –Length Prefix encoding of) the index of where the transaction sits in the atom. Mined atoms are never updated; and the position of the transaction in an atom is permanent.

### 4. Transaction Storage

**Transactions** are cryptographically signed instructions usually associated with  $\Omega$  addresses. Using  $\alpha$  scheme, a user can spend one (or more, via splitting) of their current **transaction balance** by creating a **transaction** and adding one (or more, via merging) of their current **transaction balance** as the **transaction’s** input.

During data storage, we have to keep track of the details of transaction balances, transaction states, and what happens between the two. The state of atomchain balances is represented by its global collection of both  $\alpha$  and  $\Omega$  address transaction balances. The transfer of cryptocurrency value is done through transaction balances stored (in atomchain) and propagated on atom network.

Atomchain transaction storage has only one global state trie which updates continually. This trie contains a key and value pair for every  $\Omega$  address that exists on the atom network. A World State Trie is a mutable data-structure capturing the most recent state of the atomchain. World State Trie contains a mapping between  $\Omega$  addresses and state information about them, i.e. paths in this trie link records with quarks information.

### 5. Benefits of $\alpha$ and $\Omega$ address schemes

- **Privacy:** There is a higher level of privacy as long as users use new address for each payment transaction.
- **Scalability:** Processing of multiple  $\alpha$  addresses enables parallel transactions and avenue for scalability.
- **State/Stateless Efficiency:** Transactions involving different tasks that require (or involve) state information or does not require (nor involve) state information can be processed simultaneously.

For instance, at any given point in time, if one makes **X**  $\alpha$ -based transaction and **Y**  $\Omega$ -based transaction in such a way that there is no transaction replication, and **X** and **Y** are mutually exclusive. Then the efficiency of the atomchain payment system increases by combining **X** and **Y** transactions in an atomsphere.

## 6. Formal Definition of Atomchain Payment System

A formal definition of the data structure and processes of basic atomchain payment helps in formulating frameworks for digital tokens and accounts on the atomchain.

Let  $U$  denote the set of all users of an atomchain payment system

Let  $O$  denote the set of all payment objects issued

Let  $R$  denote the set of real numbers

Let  $u_i$  be the user making the payment (sender)

Let  $u_j$  be the user receiving the payment (recipient)

- **Alpha  $\alpha$  Formalism:**

The storage (or memory) size of an alpha system is  $|\{o_k\}|$ , and it is proportional to the total number of payment objects ever issued.

The global state of an alpha system at any time instant  $t$  is given by:  $\alpha^t = \{(o_k, u_i) : o_k \in O, u_i \in U\}$

An alpha payment transaction is a 3-tuple given by:  $T = (u_i, u_j, o_k)$

where the payer ( $u_i$ ) pays (or sends money to) the payee ( $u_j$ ) a payment object ( $o_k$ ) at time  $t$ .

To process the transaction  $T(u_i, u_j, o_k)$ , the global state is updated as follows:

$$\alpha^{t+1} = \{\alpha^t \setminus \{(o_k, u_i)\}\} \cup \{(o_k, u_j)\}, \text{ where } u_i \text{ and } u_j \text{ are storage records}$$

Where  $\alpha^{t+1}$  is the new global state, and the value of the payment object  $o_k$  remains unchanged while its ownership has been transferred from the payer ( $u_i$ ) to the payee ( $u_j$ ).

During ownership transfers, splitting and merging can occur. These processes can result in a change of value of a resulting payment, as well as a change in the total number of payment objects in the global state of the alpha system.

To process a splitting alpha transaction, the global state is updated as follows:

$$\text{split: } \alpha^{t+1} = \{\text{split: } \alpha^t \setminus \{(o_k, u_i)\}\} \cup \{(o_x, u_j), (o_y, u_i)\}$$

In the splitting transaction, a user ( $u_i$ ) pays a portion ( $o_x$ ) of the value of their payment object  $o_k$  to another user ( $u_j$ ) resulting in a new payment object ( $o_x$ ) under the ownership of ( $u_j$ ) and user ( $u_i$ ) receives the remainder ( $o_k - o_x$ ) which is another payment object  $o_y$  under ( $u_i$ ) ownership.

To process a merging alpha transaction, the global state is updated as follows:

$$\text{merge: } \alpha^{t+1} = \{\text{merge: } \alpha^t \setminus \{(o_x, u_i), (o_y, u_i)\}\} \cup \{(o_z, u_j)\},$$

where  $(o_x + o_y \leq o_k)$ ,  $o_k$  is the total payment object of  $u_i$

In the merging transaction, a user  $u_i$  uses two payment objects  $o_x$  and  $o_y$  under  $u_i$  ownership to pay another user  $u_j$ . The payment objects  $o_x$  and  $o_y$  are now merged into a new payment object  $o_z$  under  $u_j$  ownership.

- **Omega  $\Omega$  Formalism:**

The storage (or memory) size of an omega system is  $|\{u_i\}|$ , and it is proportional to the total number of accounts recorded in the system.

The global state of an omega system at any time instant  $t$  is given by:

$$\Omega^t = \{(u_i, b_i) : u_i \in U, b_i \in R\},$$

Where  $b_i$  is the account balance of user  $u_i$ .

An omega payment transaction is a 3-tuple given by:

$$T = (u_i, u_j, x)$$

Where the payer ( $u_i$ ) pays (or sends money to) the payee ( $u_j$ ) an amount (in  $x$  units of value) at time  $t$ .

To process the transaction  $T(u_i, u_j, x)$  the global state is updated as follows:

$$\Omega^{t+1} = \{\Omega^t \setminus \{(u_i, b_i), (u_j, b_j)\}\} \cup \{(u_i, b_i - x), (u_j, b_j + x)\}, \text{ where } (b_i \geq x)$$

Where  $\Omega^{t+1}$  is the new global state, and the account balance ( $b_i$ ) of  $u_i$  is debited (by  $x$  amount) and the account balance ( $b_j$ ) of  $u_j$  is credited (by  $x$  amount). In this scheme, to avoid bad situations such as multispending,  $b_i$  must be equal or greater than  $x$ .

## 7. Steps in creating $\alpha$ and $\Omega$ atom wallet addresses:

- **Creating  $\alpha$  Addresses:**

1. A random string of home consisting of 64 (hex) characters (256 bits / 32 bytes) is generated first, it can be any number between 0 and  $\leq n-1$ , where  $n$  is a constant ( $n = 1.1578 * 1077$ ).
2. A string of 256-bit number which is less than  $n$  is fed to the SHA256 hashing algorithm which then generates a new 256-bit number. This is our home.
3. A 128 (hex) character (64 bytes) world is then derived from the generated home. It has '04' as the prefix. The world is generated from the home using secp256k1, which is a curve of ECDSA (Elliptic Curve Digital Signature Algorithm). So a world is generated using a formula  $P = h * G$ , where  $h$  is the home and  $G$  is the generator point. The generator point  $G$  is a defined point on the secp256k1 curve.
4. An address of 34 characters is generated by applying the SHA256 hashing algorithm on the world, then computing the RIPEMD160 hash of the result.  $A = \text{RIPEMD160}(\text{SHA256}(w))$ , where  $w$  is the world, and  $A$  is the  $\alpha$  address.  $\alpha$  addresses are always encoded as Base58Check which uses 58 characters (Base58 number system), and a checksum to avoid ambiguity, errors in address transcription, and to aid in human readability.

- **Creating  $\Omega$  Addresses:**

1. A random home of 64 (hex) characters (256 bits or 32 bytes) is generated first.
2. A 128 (hex) character (64 bytes) world is then derived from the generated home using Elliptic Curve Digital Signature Algorithm (ECDSA). An elliptic curve is a curve defined by the equation  $y^2 = x^3 + ax + b$  with  $a$  and  $b$  chosen.
3. The Keccak-256 hash function is then applied to (128 characters or 64 bytes), the world, to obtain a 64 character (32 bytes) hash string.
4. The last 40 characters or 20 bytes of this string prefixed with 0x becomes the final  $\Omega$  address.

In other words, by applying the ECDSA to the home, we get a 64-byte integer, which is two 32-byte integers that represent X and Y of the point on the elliptic curve, concatenated together.  $\Omega$  address is created by applying Keccak-256 to the home and then taking the last 20 bytes of the result.

#### 4. $\alpha$ Addresses in an Atom Wallet using JavaScript Programming Language:

$\alpha$  atom wallets are not stored in atomchain. Rather, they are managed by each individual user and referenced in individual transactions. The wallet consists of the following parts, which are generated in the same order:

- Home
- World
- World hash (WH)
- Worldaddress or
- Home WIF (wallet import format: a standard introduced to make it easier and more secure for users to migrate wallets from different services.)

**Create a home.** A home is a 32-byte array in binary. Since there are 8 bits in a byte, that makes 256 bits.

The JavaScript code:

```
const secureRandom = require('secure-random');
let home = secureRandom.randomBuffer(32);
console.log('> Home created: ', home.toString('hex'));
```

**Note:** Only homes that are less than the following value (in hexadecimal) work with  $\alpha$  atom wallets: 0xFFFF FFFF FFFF FFFF FFFF FFFF FFFF FFFF BAAE DCE6 AF48 A03B BFD2 5E8C D036 4140.

This is because atomchain uses elliptic curve cryptography (ECC) and can only accept homes below that number. The version of elliptic curve cryptography that atomchain uses is called `secp256k1`

The JavaScript code now becomes:

```
const max =
Buffer.from("0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFEBAAEDCE6AF48A03BBFD25E8CD03641
40", 'hex');
let isInvalid = true;
let home;
while (isInvalid) {
  home = secureRandom.randomBuffer(32);
  if (Buffer.compare(max, home) === 1) {
    isInvalid = false;
  }
}
console.log('> Home: ', home.toString('hex'));
```

We use a `while` loop to keep generating homes until we find one that is below that `max` amount. That shouldn't be hard, since `max` is fairly close to  $2^{256}$ .

**Create a world.** We will make use of the `elliptic` JavaScript library to generate our world.

The JavaScript code:

```
const keys = ecdsa.keyFromPrivate(home);
const world = keys.getPublic('hex');
console.log('> World created: ', world);
```

**Generate a world hash.** Here, we run the world through both the SHA-256 hashing algorithm and the RIPEMD-160 hashing algorithm.

The JavaScript code:

```
const sha256 = require('js-sha256');
const ripemd160 = require('ripemd160');

let hash = sha256(Buffer.from(msg, 'hex'));
let worldHash = new ripemd160().update(Buffer.from(hash, 'hex')).digest();
```

**Generate a world address.** We first add the prefix “00” in hex to our world Hash. Then we derive the SHA-256 hash of the extended world hash. Then we derive the SHA-256 hash of that and store the first byte as a “checksum.” We add the checksum to the extended world hash and encode it with base 58.

The JavaScript code:

```
function createPublicAddress(worldHash) {
  // step 1 - add prefix "00" in hex
  const step1 = Buffer.from("0x00" + worldHash, 'hex');
  // step 2 - create SHA256 hash of step 1
  const step2 = sha256(step1);
  // step 3 - create SHA256 hash of step 2
  const step3 = sha256(Buffer.from(step2, 'hex'));
  // step 4 - find the 1st byte of step 3 - save as "checksum"
  const checksum = step3.substring(0, 8);
  // step 5 - add step 1 + checksum
  const step4 = step1.toString('hex') + checksum;
  // return base 58 encoding of step 5
  const address = base58.encode(Buffer.from(step4, 'hex'));
  return address;
}
```

**Generate a home WIF.** Here are the steps:

- We add a prefix to the home. In this case it is “80” (in hexadecimal)
- We derive the SHA-256 hash of the extended home.
- We derive the SHA-256 hash of that, and then save the first byte as the checksum.
- We add the checksum to the extended home and encode it to base58.

The JavaScript code:

```
function createhomeWIF(home) {
  const step1 = Buffer.from("80" + home, 'hex');
  const step2 = sha256(step1);
  const step3 = sha256(Buffer.from(step2, 'hex'));
  const checksum = step3.substring(0, 8);
```

```

const step4 = step1.toString('hex') + checksum;
const homeWIF = base58.encode(Buffer.from(step4, 'hex'));
return homeWIF;
}

```

In other words, the checksum is created by hashing the home, and taking the first 4 bytes of the result. So you cannot get the valid  $\alpha$  address without adding the checksum bytes.

### 5. Implementing $\Omega$ Addresses in an Atom Wallet using Python Programming Language:

```

home_bytes = codecs.decode(home, 'hex')
# Get ECDSA public key
key = ecdsa.SigningKey.from_string(home_bytes,
curve=ecdsa.SECP256k1).verifying_key
key_bytes = key.to_string()
key_hex = codecs.encode(key_bytes, 'hex')

world_bytes = codecs.decode(world, 'hex')
keccak_hash = keccak.new(digest_bits=256)
keccak_hash.update(world_bytes)
keccak_digest = keccak_hash.hexdigest()
# Take the last 20 bytes
wallet_len = 40
wallet_address = '0x' + keccak_digest[-wallet_len:]

```

An  $\Omega$  address in fact, is a 160-bit (20 bytes) identifier, which is created as last 20 bytes of a world from the user signature. Adding a checksum to this address makes it case-sensitive. The Python code for this checksum is as follows:

```

checksum = '0x'
# Remove '0x' from the address
address = address[2:]
address_byte_array = address.encode('utf-8')
keccak_hash = keccak.new(digest_bits=256)
keccak_hash.update(address_byte_array)
keccak_digest = keccak_hash.hexdigest()
for i in range(len(address)):
    address_char = address[i]
    keccak_char = keccak_digest[i]
    if int(keccak_char, 16) >= 8:
        checksum += address_char.upper()
    else:
        checksum += str(address_char)

```

- 6. Notes:** You lose everything in your world if you lose your home. Protect your home from the internet by keeping your home safely intact offline. Your home is the only access to your world