Crypto.com Chain: The next generation decentralized mobile payment protocol

{chain,contribute}@crypto.com

September 17, 2019
v0.5.0

Abstract

The development of blockchain technology and cryptocurrencies represent a cryptography and security breakthrough as significant as that created by the internet in the 1990s. This technology, however, is still at a very nascent stage; in order to generate mass adoption, it will therefore be necessary to find compelling real-life use cases that can appeal to an audience larger than the small group of industry professionals and experts. We believe that enabling cryptocurrency spending in the real world will constitute an adoption catalyst. Current traditional payment institutions and existing blockchains have failed to provide a secure, scalable and decentralized solution to support cryptocurrency payment.

Accordingly, we propose Crypto.com Chain, the next generation decentralized mobile payment protocol, the most efficient and secure way to pay and be paid in crypto, anywhere, any crypto at little to no cost. Crypto.com Chain will deliver on its vision by developing innovative technology components and processes (inc. scalable encryption algorithm to protect users privacy, utilizing trusted execution environments, sustainable price stability mechanisms, user protection via PoGSD) catered specifically to cryptocurrency payment, while leveraging proven blockchain technology structural design elements.

Table of Contents

1. Introduction to Crypto.com Chain

Current traditional payment infrastructure and existing blockchain-powered payment networks have failed to provide a wide-spread, easy-to-integrate and fast settlement of cryptocurrency in the real world.

The key limitations of existing payment network infrastructures are that they:

1. Do not integrate with cryptocurrencies systematically;
2. Do not give access to either customers or merchants a way to reconcile the numbers in a trustless way;
3. Are vulnerable due to being the central point of failure;
4. Are expensive to operate;
5. Give low limits on cryptocurrency spending by default;

Moreover, the key limitations of existing blockchain-powered payment networks are that they are:

1. Too complex to setup and use;
2. Not friendly to crypto first timers;
3. Rarely supported beyond their own blockchain;

Our vision is to accelerate the world's development, adoption of and transition to cryptocurrency. Crypto.com Chain is the best way to pay and be paid in crypto, anywhere, anytime and using any crypto — at little to no cost.

2. Design Axioms

Crypto.com Chain, the next generation decentralized mobile payment protocol, will be designed based on the following foundational Design Axioms (DA_n), listed in order of priority ($DA_i > DA_{i+1}$):

DA_1: Secure
- Protect from fraud;
- Highly compliant.

DA_2: Highly Scalable & Fast
- Peak performance on par with centralized payment providers;

- Fast confirmation; targeting < 1 second through different means (e.g. P2P payment channels).
- High transactions per second (TPS); targeting 50,000 TPS, through different means (e.g. P2P payment channels);

DA_3: Augmented Decentralization

- Self-managed settlement;
- Phased validator node set evolution;
- Automated treasury rewards and sequencing.

DA_4: Upgradable and Fast In Innovation

- Flexible process for chain upgrades;
- Low dependency on other networks.

DA_5: Data Privacy Protection

- Encrypted on-chain pseudonymous transaction data, only relevant parties involved in each transaction can decrypt it;
- Efficient transaction validation.

DA_6: Inclusive

- Seamless integration of new acquirers or customer/merchant with low technical barriers, appropriate incentives and strict penalties.

Decentralized ledger technology, such as blockchain, provides key built-in benefits that are aligned with Crypto.com Chain Design Axioms:

- it handles double spend naturally,
- it makes reconciliation easier, (it even 'removes' the need for reconciliation, as long as the blockchain is properly structured),
- it facilitates open collaboration,
- it is more inclusive, anyone can join the network,
- it lowers the likelihood of central point of failure.

3. Architecture

Overview

Building a blockchain is not just about software/hardware development. Rather, it is a combination of technological design, incentive mechanism, game

theory and governance, which together nourish a robust system that also allows for continuous innovation. Our initially proposed architecture may hence undergo future revisions in response to changes in incentives, governance or other external requirements.

As Crypto.com Chain is intended for mobile payments, our proposed architecture needs to reflect the inherently federated nature. The network consists of nodes arranged in different layers, each of which is designed to serve the different needs of different users. This architecture is proposed in line with our Design Axioms where DA_1 and DA_2 are of the highest priority.

The different node types, their permissions and responsibilities are summarised in the table below.

Node type	Who can run it?	Rights and obligations	Requirements
Council Nodes	Initially, Crypto.com Chain servers. This will be split and extended to third-party entities as the network scales, based on minimum staking requirements and tier-based randomised selection	Council Nodes have the following rights and obligations: • Executing settlement; • Maintaining a whitelist log of Council Node identities; • Maintaining a whitelist log of Acquirer Node identities; • Maintaining a whitelist log of Settlement Agent Node identities; • Ordering transactions and reward CRO in a limited supply; • Verifying all transactions; • Sending/receiving transactions; • Reading data.	• Post CRO collateral; • Dedicated IP; • Meeting the infrastructure requirements; • Compliance with the privacy policy. *A minimum number of Council Nodes will be deployed across the globe.
Acquirer Nodes	Customer acquirers, Merchant acquirers.	Acquirer Nodes have the below rights and obligations: • Settle on behalf of others; • Provide an escrow ("Proof of Goods & Services Delivered") service; • Provide a verified merchant name mapping service;	• Post CRO collateral; • Dedicated IP, *Each acquirer is advised to run multiple nodes to achieve business continuity.

		• Send/receive transactions; • Verify related transactions; • Read data,	
Settlement Agent Nodes	Anyone who has the capability to settle between CRO and currencies deemed stable	Settlement Agent Nodes have the below rights and obligations: • Sell CRO for other currencies deemed stable; • Settle for oneself; • Send/receive transactions; • Verify related transactions; • Read data.	• Post CRO collateral.
Community Nodes	Anyone.	Community Nodes have the below rights and obligations: • Settle for oneself under certain conditions; • Send/receive transactions; • Verify related transactions; • Read data.	• Optionally post CRO collateral.

Crypto.com Chain is open to the public to join, participate and scrutinise related transactions. We do not expect that, for example, mobile clients will be able to perform heavy-lifting tasks and have a reliable always-online network connection. For that reason and DA_2, the capabilities of Community Nodes are different from those of other node types.

Trusted Execution Environments

In order to address DA_1, DA_2, DA_3, and DA_5, the core functionality of Crypto.com Chain Nodes is designed to run in secure enclaves of Trusted Execution Environments (TEEs). TEEs, such as Intel SGX, Arm TrustZone, or Keystone[1], are extended CPU instruction sets that isolate code executed in an enclave from the host operating system in hardware-encrypted RAM. TEEs ensure that even the node administrator cannot see private data that enclave code works with. Note that enclave code must still follow secure coding practices in order to avoid leaks through memory access patterns etc.

An important feature of TEEs is their local and remote attestation. This feature enables nodes or external parties to verify that the code they plan to

[1] An ongoing open-source project for RISC-V: https://keystone-enclave.org

interact with is indeed the certified Crypto.com Chain code. In case of remote attestation, each node completes this step before establishing secure communication channels with other nodes.

In Crypto.com Chain design, TEEs can find several compelling use cases:

1. Sealing ledger data: While all transaction data can be distributed to any node for processing, humans (even node administrators) cannot view these data in their raw form.
2. "Virtual" hardware wallets: Community nodes can utilize Ledger Trustlet[2]-like software to protect their private keys.
3. Payment protocol enhancements: TEEs have gained popularity in blockchain systems research, as they can offer high transaction throughputs with low latency.
4. Witnessing external data: For data from oracles or other blockchain networks, TEEs can be used to attest data authenticity.

In the light of Foreshadow[3] attack, Crypto.com Chain will not rely solely on TEEs for achieving DA_1 and DA_5 , we will also consider other measures, including the following:

- Double attestation scheme: As employed by Tesseract[4] decentralized exchange, this scheme protects against potential weaknesses in TEE remote attestation;
- CRO collaterals;
- Additional cryptographic measures for maintaining privacy;
- Writing core parts in Rust[5,6], a programming language that ensures memory safety and freedom of data races.

Consensus

Council Nodes run a Byzantine Fault Tolerant (BFT) consensus protocol among themselves which resolves the final order of transaction sequences. The

[2] https://github.com/LedgerHQ/bolos-tee

[3] https://foreshadowattack.eu

[4] https://eprint.iacr.org/2017/1153.pdf

[5] https://github.com/baidu/rust-sgx-sdk#rust-sgx-sdk

[6] https://edp.fortanix.com

initial prototype will utilize the Tendermint Core[7] consensus engine. Tendermint works well for PoS / PoA networks, allows high transaction throughputs, and provides instant transaction finality on block commitment, which aligns well with DA_2. It was chosen as the consensus engine for the Chain prototype due to the following additional reasons:

- **Backed by formal research**[8];
- **Robustly tested implementation**[9];
- **Track record of adoption**[10], including Binance DEX;
- **Modular architecture**.

In addition to transaction ordering, Council Nodes maintain a transparent audit log of Merchant Acquirer, Customer Acquirer, and Council Node identity changes (external gateway IPs, public key certificates etc.). Whenever a Node identity is added, updated or revoked according to a specified policy, at least 67% of Council Nodes need to approve this change.

To ensure a decentralized and robust audit log, we will explore the use of a skipchain, a shared authenticated data structure proposed in Chainiac[11]. Moreover, to facilitate a high availability, the total number of Council Nodes in different locations will be required to be greater than a minimum set that is based on real performance tests.

Governance

Council Nodes are responsible for the governance of the network. The Crypto.com Chain Entity will propose software upgrades for approval by Council Nodes. Following a software upgrade approval and release, any nodes on the network that fail to upgrade after a specified grace period will be considered as having dropped out of the network voluntarily.

Security

As it is a public network, security (DA_1) and robustness are critical requirements. Threat modeling is a systematic approach to find potential

[7] https://tendermint.com
[8] https://eprint.iacr.org/2018/574.pdf
[9] http://jepsen.io/analyses/tendermint-0-10-2
[10] https://forum.cosmos.network/t/list-of-projects-in-cosmos-tendermint-ecosystem/243
[11] https://eprint.iacr.org/2017/648.pdf

threats by decomposing and enumerating system components. There are many different methodologies and/or frameworks when conducting threat modeling, such as STRIDE, DREAD, Attack Tree, etc. In our case, our Threat Model is based on STRIDE and Attack Tree.

STRIDE provides a set of security threats in six categories:

1. **Spoofing**: Impersonating the identity of another
2. **Tampering**: Data is changed by an attacker
3. **Repudiation**: An attacker refuses to confirm an action was conducted
4. **Information Disclosure**: Exposing sensitive information
5. **Denial of Service**: Degrade the availability or performance of the system
6. **Elevation of Privilege**

For each category, we enumerate all the potential threats by breaking down a high-level goal into more specific sub-goals, in a way similar to attack tree enumeration. And in each sub-goal, we set the risk level by combining the Severity and Exploitability of the item.

Severity

- **5**: Severe impact on the whole system
- **4**: High impact on the whole system
- **3**: Moderate impact on the whole system or Severe impact on individual user/node
- **2**: High impact on individual user/node
- **1**: Moderate impact on individual user/node

Exploitability

- **5**: Existing exploit code available
- **4**: Relatively easy to exploit
- **3**: Attack is practical but not easy, a successful attack may require some special conditions
- **2**: Theoretically possible, but difficult in practice
- **1**: Very difficult to exploit
- **0.1**: Almost impossible

Assets

1. **The integrity of the account balance**: the most important piece of information in the blockchain.

2. **Validator secret keys** (block-signing keys of Council Nodes): one of the most powerful keys, lost 1/3 of these keys will render the whole system to an unstable state.
3. **User secret keys**: key owner implies fund owner
4. **Transaction encryption keys**: transaction privacy of the system relies on the secrecy of this key

Scope

The whole Crypto.com Chain is a complex system and involves many different components. And therefore, the scope of this threat model is limited only to the major components of the system. To be more specific, the threat modeling of Tendermint and Intel SGX is not in the scope of this threat modeling.
We also assume standard security measures such as OS level hardening, software patching, anti-virus, network firewalls, physical security etc. are properly implemented, executed and monitored. These mitigation strategies are not mentioned here.

Threat Model

The initial threat model can be found here.

Privacy

As TEEs are used, the data inside secure enclaves is protected; even the node administrators cannot directly view raw transaction data on their nodes.

To further enhance privacy capabilities (addressing DA_1 and DA_5), Crypto.com Chain will include other software-based measures in case of secure enclave breaches. The initial prototype will utilize tree signatures[12] for threshold multi-signatures which provide a good trade-off between privacy and accountability. Furthermore, we will potentially explore employing other techniques, such as additively homomorphic commitments (as used, for example, in Confidential Transactions[13]), where data remains private even in the case of secure enclave breaches, and its processed parts can be securely and verifiably exposed for third-party auditing.

[12] https://blockstream.com/2015/08/24/treesignatures/
[13] https://people.xiph.org/~greg/confidential_values.txt

Compliance

Onboarding of Customer and Merchant Acquirers

Customer Acquirers and Merchant Acquirers are onboarded only if they are able to pass the Crypto.com KYC check[14] and comply with KYC standards when they onboard downstream customers and/or merchants.

As mentioned in the Consensus section, CRO may utilize a Chainiac[15]-style skipchain for robust and decentralized audit logging. Acquirer Nodes' KYC check metadata, identities and policies for updating associated keys will be stored in an entry on the skipchain.

Consumers and merchants (through Community nodes) will also be able to have an entry attesting their identity on the skipchain after passing KYC (performed by Acquirer or Crypto.com Chain Entities). The associated keys could be stored in the user's mobile phone or other devices that interact with the CRO network. Merchants whose access is provided through Merchant Acquirer Nodes may maintain their real world identity by linking their existing X.509 certificates.

The associated private keys can be securely stored in the TEE of the mobile device and interacted with via the CRO Mobile Wallet App. In this way, private keys of consumers and merchants cannot be directly read and can only be used in a restricted way via mobile app interactions with the "virtual" hardware wallet.

Certain transaction types may require the wallet address to be associated with a valid entry in the skipchain. In the scenario where a mobile device is lost, the corresponding Acquirer or Crypto.com Chain Entity would be able to update the skipchain entry according to the set policy. The consumer or merchant will either restore the corresponding wallet on a new device or request an identity update with a new associated key pair.

Crypto.com Chain Entity and Acquirer nodes will be responsible for updating or revoking corresponding identities on the skipchain.

[14] Or in future, pass KYC check of any entity that runs other services.

[15] https://eprint.iacr.org/2017/648.pdf

4. Settlement & Price Stability

Routed & Direct Settlement

Routed Settlement

For transactions conducted through Acquirer Nodes, the acquirers will be responsible for settling the funds downstream with customers (debit) and merchants (credit).

Direct Settlement

Customers and merchants who establish their own Community Nodes, and who have enough CRO staked and registered Settlement Accounts will be able to settle directly through the Crypto.com Chain, with the same float account requirements and rules as Acquirers Nodes.

This settlement option provides several benefits:

1. **Faster downstream settlement:** the moment the counterparty settles, the customers and merchants with Community Nodes will settle automatically;
2. **Inclusive network:** enabling anyone to leverage the power of the Crypto.com Chain network;
3. **Transparency:** even for Community Nodes that do not meet the settlement requirements but have declared linkage to one of the Acquirer Nodes, they would be able to witness all (encrypted) transactions going through the Crypto.com Chain Network and decrypt those that concerning them. As a result, customers and merchants will not have to rely on acquirers' report to check whether a transaction has been processed.

The escrow service, "Proof of Goods & Services Delivered" (PoGSD), will rely on the multi-signature wallets and collaterals in the CRO Protocol. If a customer decides to pay a merchant without a collateral or who is not on the CRO network, the CRO Mobile Wallet App will display a warning that PoGSD is not available before the transaction occurs.

Settlement Agents

Cryptocurrency asset class is nascent and volatile. Merchants are however looking for price stability to manage and forecast their PnL.

To increase cryptocurrency acceptance among merchants, it is key to be able to provide them with price stable conversion post-settlement options. Settlement Agents will perform this service via CRO currency conversion to currencies deemed stable (transaction details including rates will be recorded on-chain; settlement will happen off-chain).

To become eligible, Settlement Agents will need to:

1. Guarantee at least better conversion rate than the Crypto.com Chain benchmark[16] for a defined period of time; and
2. Stake CRO tokens.

Settlement Agents will receive CRO tokens in exchange for other currencies at settlement times. The extra amount would be added to the 2-of-3 lock setup during the exchange process and used as an escrow fee payment in the case of disputes.

Settlement Currencies

All transactions on the Crypto.com Chain are performed using the native blockchain token CRO. As a customer, you will be able to pay using any cryptocurrency paired with CRO. Following the transaction authorization, the customer acquirer will deduct the equivalent CRO amount in your selected cryptocurrency wallet for future settlement with the merchant.

As a merchant, you will be paid by default in CRO tokens, however, you will have the ability to convert on the spot to currencies deemed stable (inc. stable coins and fiat currencies). Settlement Agents (detailed below) will perform the conversion for merchants and hedge their risk. Settlement time is expected to be around T+0 for crypto conversion and T+2 for fiat conversion.

[16] This benchmark will be likely be calculated using a verified external price source collected using an oracle.

Settlement Process

Each Acquirer, Community[17] or Settlement Agent Node[18] can maintain their balances by processing blocks that include transactions relevant to them. Transaction relevance can be checked using a fixed-sized probabilistic filter, which tags each block.
In the absence of a Settlement Agent, a customer or his/her acquirer can directly send a transaction that outputs an amount locked for a corresponding merchant and its acquirer. Depending on the situation, the customer may optionally choose to lock the output with a threshold condition using the escrow service.

Using a Settlement Agent introduces a counterparty risk between Settlement Agents and Merchant Acquirers. This risk is mitigated in the following ways:

- Merchant Acquirer nodes maintain a whitelist of Settlement Agents. This allows Merchant Acquirers to choose among Settlement Agents they trust.

- Involved parties will follow this settlement flow:
  (1) Customer sends CRO to a Customer Acquirer or to a Merchant Acquirer (depending on the setup).

  (2) Customer Acquirer locks CRO in a multi-signature address, which can release the CRO to the Settlement Agent when 2 out of 3 signatures (Settlement Agent signature, Merchant Acquirer signature, Escrow Agent signature) are met.

Scenario A - "The good flow":

(A3) Settlement Agent sends corresponding fiat (e.g. USD) to Merchant Acquirer.

(A4) Settlement Agent creates a transaction to release CRO and this transaction is co-signed by the Settlement Agent and Merchant Acquirer.

[17] For direct settlements

[18] For with Settlement Agent trades

(Merchant Acquirer settles with their Merchants based on their existing arrangements, e.g. on a monthly basis.)

Scenario B - Disputed by Settlement Agent :

(B3) Settlement Agent sends fiat currency to Merchant Acquirer, but the Merchant Acquirer refuses to co-sign the fund release transaction.

(B4) Settlement Agent provides proof to the involved Escrow Agent that the fiat transfer has occurred.

(B5) If the proof is satisfactory, both the Escrow Agent and Settlement Agent will sign the confirmation message to release the CRO to the Settlement Agent.

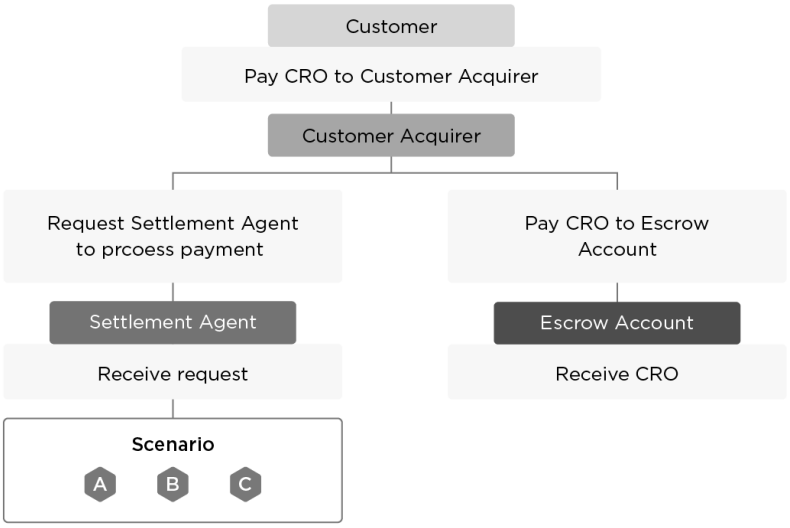
Scenario C - Disputed by Merchant Acquirer:
If the Settlement Agent fails to send fiat to the Merchant Acquirer, and this behaviour repeats several times, Merchant Acquirer could remove the Settlement Agent from its whitelist and:

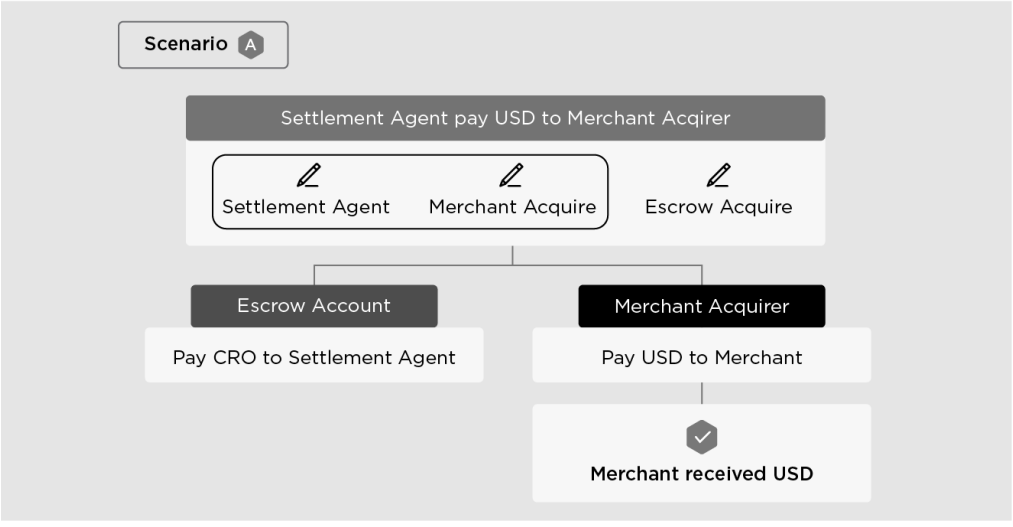
(C3) Merchant Acquirer contacts the Escrow entity.

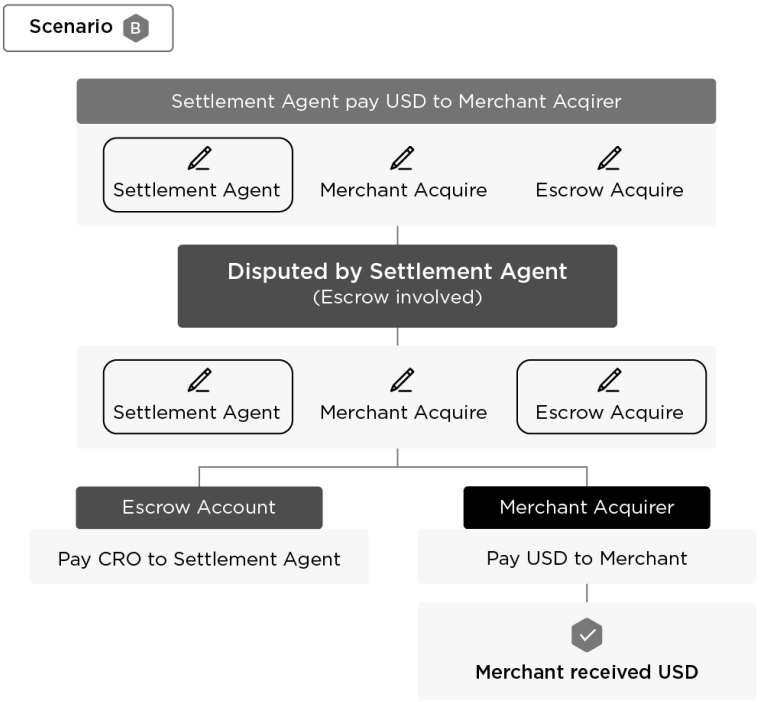
(C4) After the Escrow verifies the situation, both Merchant Acquirer and Escrow Agent create a reverse-transaction to release the CRO instead to Merchant Acquirer and co-sign the transaction.

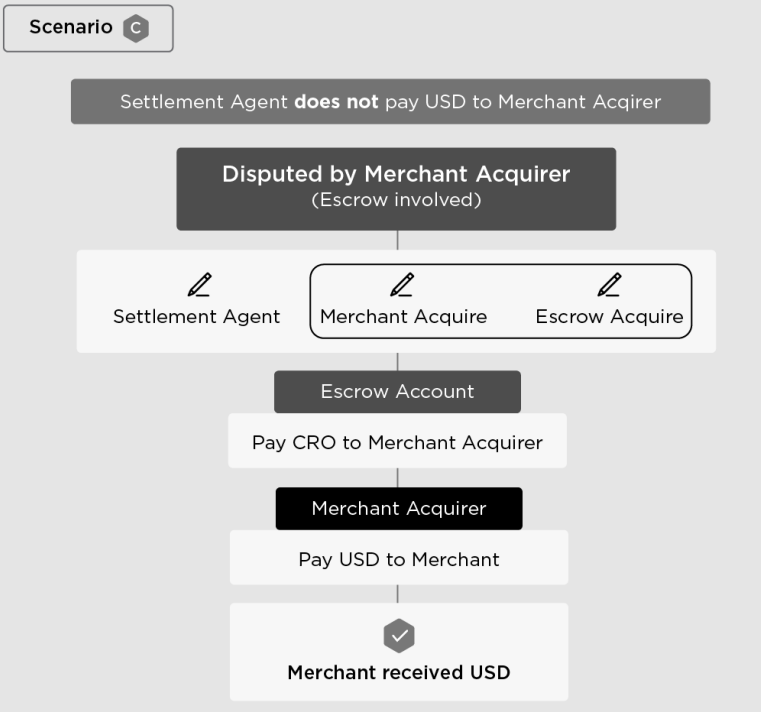
Similar flows are followed in interactions between Settlement Agents and Customer Acquirers. When other cryptocurrencies are involved, similar escrow arrangements and atomic swaps can be employed.

Transaction Flow Summary:






Scenario B
Settlement Agent pay USD to Merchant Acqirer
Settlement Agent
Merchant Acquire
Escrow Acquire
Disputed by Settlement Agent
(Escrow involved)
Settlement Agent
Merchant Acquire
Escrow Acquire
Escrow Account
Merchant Acquirer
Pay CRO to Settlement Agent
Pay USD to Merchant
Merchant received USD


Scenario C
Settlement Agent does not pay USD to Merchant Acqirer
Disputed by Merchant Acquirer
(Escrow involved)
Settlement Agent
Merchant Acquire
Escrow Acquire
Escrow Account
Pay CRO to Merchant Acquirer
Merchant Acquirer
Pay USD to Merchant
Merchant received USD

5. Block Structure & Incentives

The details described in this section, as with other technical aspects of the Crypto.com Chain, are subject to revision. The described data structures only highlight a subset of end-user metadata that will be exchanged in protocol messages among relevant nodes. The exact details, handling etc. will depend on interactions with the underlying consensus layer, privacy and security mechanisms.

Data Structure

Payment Transaction Data Structure

The accounting model in the initial prototype of Crypto.com Chain prototype will follow the UTXO model similar to Bitcoin, except that Chain's transaction output locking will be more restrictive (addressing DA_1 and DA_2). The overall accounting model is, however, a mixed version where staking-related utilize accounts (see technical documentation for details). The committed transaction included in a block will include at least these parts:

A. Raw transaction data encrypted against a verifiable shared secret of Council Nodes;
B. Hash of the raw transaction data.

Moreover, depending on the implementation, it may additionally include references to past data that needed to be fetched for transaction validation purposes.

Part A) Raw transaction data will never be revealed directly, as discussed in Privacy. The following encrypted data may contain additional obfuscation to prevent data leaks in case of TEE access policy breaches:

1. Transaction data:
    a. Transaction inputs;
    b. Transaction outputs.
2. An access policy of what can be exposed to whom, and under what circumstances, from the raw transaction data (enforced by TEEs). This access policy will refer to one-time keys related to:
    a. The customer's wallet,
    b. The merchant's wallet,
    c. The optional escrow service provider (PoGSD),
    d. Related Acquirer Nodes.

3. Transaction metadata: this includes versioning information, network identifier, and metadata related to the use of external currencies.
4. Collective witness, including signatures on the transaction's ID, against each transaction input.

To communicate transaction data across the network to related parties, interim state transactions will contain some of the above mentioned data.
In order to address DA_6, all transaction data will be serialized in a backwards and forwards-compatible way, using a well-established binary format (the initial prototype will utilize the Simple Concatenated Aggregate Little-Endian binary codec defined in Section B.1 of Polkadot RE Protocol Specification); this will help to ensure the ease and consistency of implementations across different programming languages used in third party integrations.

Transaction Flows: Proof of Goods & Services Delivered

Scenario A: The item is shipped:

A1) Normal

If the buyer confirms and accepts the delivered item, he/she can complete the purchase by co-signing the transaction to the merchant with his/her signature.

A2) Payment dispute (escrow/acquirer involved)

If the merchant has not received the payment after a certain period of time, he/she can contact and provide evidence of delivery to the escrow. Once it has been confirmed, the transaction will be co-signed by the escrow and the funds will be released to the merchant.

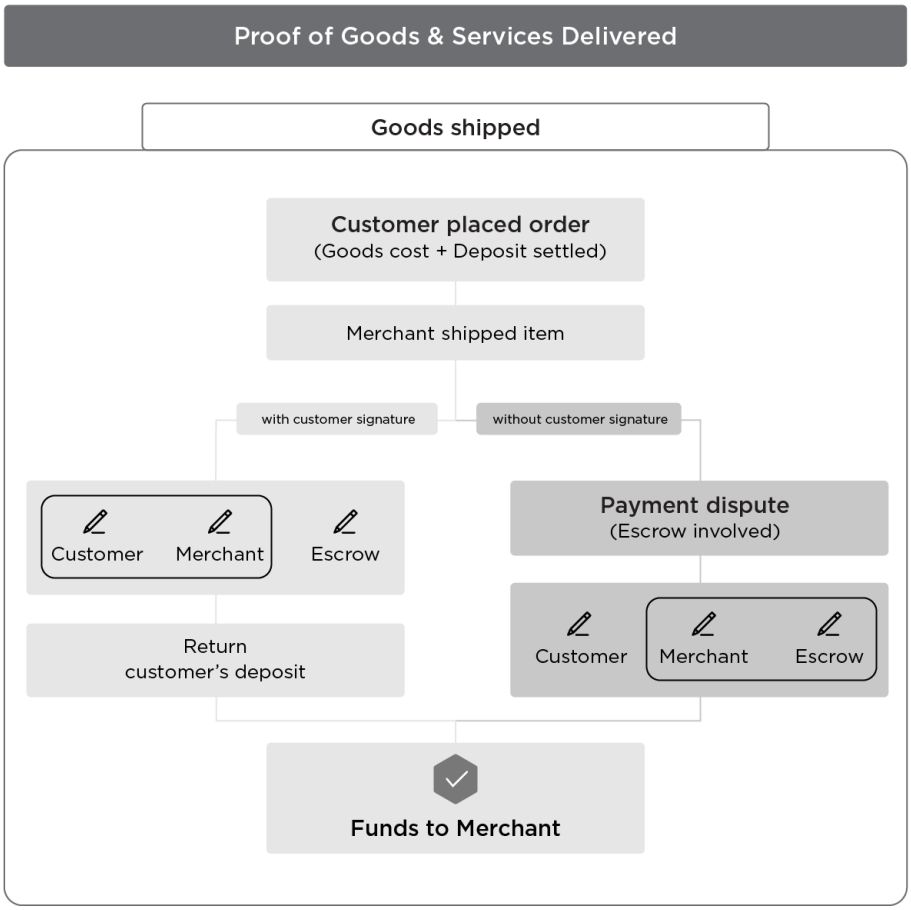
Scenario B: The item is not shipped/not as described:

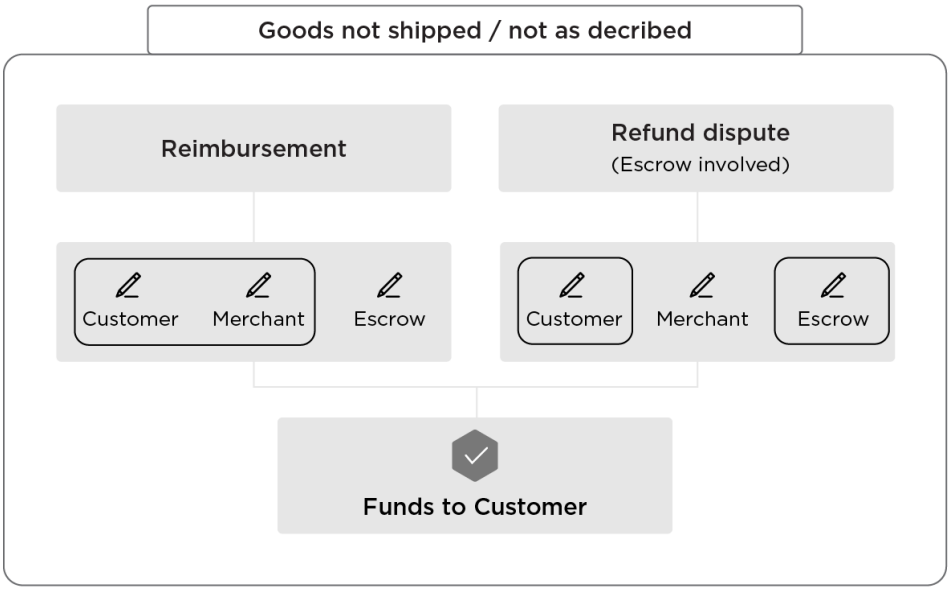
B1) Reimbursement (without escrow/acquirer involvement)

The buyer can request a refund when the merchant failed to fulfil the order. If the merchant accepts the request, he/she can co-sign the transaction and refunds the buyer.

B2) Refund dispute (escrow/acquirer involved)

In case of the merchant neither agree with the refund claim nor respond to buyer's refund request, the buyer can reach the escrow to resolve the issue. If the resolution outcome is in favour of the buyer, escrow will issue a refund to the buyer by providing the co-signature.


Proof of Goods & Services Delivered
Goods shipped
Customer placed order
(Goods cost + Deposit settled)
Merchant shipped item
with customer signature
without customer signature
Customer
Merchant
Escrow
Return
customer's deposit
Payment dispute
(Escrow involved)
Customer
Merchant
Escrow
Funds to Merchant


Goods not shipped / not as decribed
Reimbursement
Customer
Merchant
Escrow
Refund dispute
(Escrow involved)
Customer
Merchant
Escrow
Funds to Customer

Block Data Structure

As the initial prototype of Crypto.com Chain will utilize Tendermint Core as its consensus engine, the block structure will follow the descriptions provided as described in Tendermint's documentation.

Furthermore, Crypto.com Chain will employ these additional conventions:

1. AppHash consists from a root of an authenticated data structure, such as a Merkle tree[19], constructed after committing a set of valid transaction in a given block and other parts, denoting the application state. Given an AppHash portion, a transaction ID and a Merkle proof, one can verify whether a transaction corresponding to a given ID was included in a block;
2. Each block will be tagged with a fixed sized probabilistic data structure, such as a Bloom filter[20], that will encode participants from all transactions in a given block.
3. The last two characters of ChainID will be assumed to be hexadecimal digits. These encode a single byte that should be included in every transaction's metadata. This value will vary for different network deployments, such as test and main networks.

Textual Address Format

For backwards-compatibility with the existing contract on Ethereum, the staking addresses would preserve the hexadecimal textual representation.
The payment transaction addresses will utilize a new Bech32-based textual address representation where the human-readable part would denote the network (i.e. mainnet, testnet, regnet) transactions are meant for.

Transaction Fees

The network will initially have the following minimal linear transaction fee scheme: A + B*(transaction size in bytes) where A and B are constants (fractions of the native currency). These fees are paid to the rewards pool.
In the case of acquirers, these minimal fees may be subsidised.

---

[19] Merkle, R. C. (1988). "A Digital Signature Based on a Conventional Encryption Function". *Advances in Cryptology — CRYPTO '87*. Lecture Notes in Computer Science. **293**. pp. 369–378.

[20] Bloom, Burton H. (1970), "Space/Time Trade-offs in Hash Coding with Allowable Errors", *Communications of the ACM*, **13** (7): 422–426,

In the long term, we will investigate the possibility of dynamic or zero fee schemes as long as these schemes preserve the payment data confidentiality and do not open the network to spam.

Transaction Rewards

The Crypto.com Chain will extract rewards from the Secondary Distribution & Launch Incentives Pool and subsequently the Network Long Term Incentive Pool.[21]

The rewards will be periodically distributed to the Council Nodes based on their proven operation, i.e. based on the blocks they co-signed, as long as their corresponding accounts were not punished due to Byzantine faults.

Additionally, transaction rewards in the form of "cashbacks" may be paid to the acquirer customers using a faucet-like mechanism from the community development pool.

Dispute Resolution

Refund

In cases of disputes between customer and merchant, both parties will be able to leverage the Crypto.com Chain dispute resolution platform in order to agree on a win-win outcome (including refund). The dispute resolution handling is facilitated through the use of multi-signature wallets and a built-in escrow service.

Once the dispute is resolved, and if a transaction refund is agreed upon, it will be settled on-chain as a transaction that is constructed and co-signed by Customer/Merchant Acquirer.

Double-spending

[21] See the Crypto.com Chain general whitepaper for details on CRO token distribution split.

The consensus algorithm and cryptographic measures are set up to ensure that double-spends are prevented by the network protocol, as long as 2/3 of Council Nodes are honest.

6. Resilience & Agility

Network Redundancies

To ensure the robustness of the network, a minimum number of Council Nodes spread across the globe will need to be up and running. The minimum number will be decided based on real performance tests to balance the following factors:

1. robustness against compromising a supermajority of Council Nodes;
2. efficiency/high-performance.

Network Scalability & Performance

Crypto.com Chain aims to be a distributed network that is able to handle high transaction throughputs and low latency. Scalability and performance are hot research topics in the blockchain space. While adopting TEEs in the infrastructure may achieve a performant network, we will also explore other advances in the field, including sharding, consensus protocol improvements, transport network enhancements etc.

Transaction signatures will employ both ECDSA (for backwards compatibility) and a variant of the Schnorr signature scheme[22]. The Schnorr signature scheme has been recently proposed for the Bitcoin network[23]. One of the most compelling applications of this scheme thus far is compact multi-signatures, as n-of-n signatures are no different from ordinary signatures from the verifier's perspective (the same scheme is used).

In later phases, Crypto.com Chain may incorporate more recent developments from the blockchain research space in order to meet its network scalability and performance demands.

---

[22] C.P. Schnorr (1990), "Efficient identification and signatures for smart cards", in G. Brassard, ed. *Advances in Cryptology—Crypto '89*, 239-252, Springer-Verlag. Lecture Notes in Computer Science, nr 435

[23] https://github.com/sipa/bips/blob/bip-schnorr/bip-schnorr.mediawiki

One such development direction relates to the blockchain compression approaches. For instance, Coda[24] is a proposed cryptocurrency protocol which that introduces a "succinct blockchain". Instead of storing the entire transaction history, as in the current blockchain systems, it constructs a constant-sized cryptographic proof of the validity of blockchain state; this is accomplished through the recursive composition of zk-SNARKs. Coda promises to reduce the enormous blockchain sizes from hundreds of GBs or TBs to merely a few KBs.

Furthermore. when bootstrapping procedures are developed for Tendermint Core, Crypto.com Chain may allow for the safe snapshotting and pruning of historical data that is unneeded for transaction validation.

Crypto.com Chain will initially use the standard network protocol stack (such as TCP+TLS) for different node-to-node communications. Depending on the performance needs, the later Crypto.com Chain phases may explore other options. For example, QUIC[25] is a recent protocol standard proposed by Google on top of UDP that improves over TCP and TLS. QUIC can achieve better network latencies than TCP and TLS thanks to various features, such as faster connection opening and negotiation, out-of-order packet delivery or forward error correction.

[24] https://cdn.codaprotocol.com/v2/static/coda-whitepaper-05-10-2018-0.pdf

[25] https://datatracker.ietf.org/doc/draft-ietf-quic-transport/

Lightweight client support

We also provide support to lightweight clients: By connecting to a full note that has access to the complete blockchain, only a small part of the blockchain has to be downloaded and verified by the lightweight client. This allows lightweight users to access and interact with the blockchain without having to synchronise the entire blockchain. As a result, clients will be able to perform/verify payments in cryptocurrency using a mobile wallet on devices operating under resource constraints, such as smartphones or laptops.

Upgrading the Network

Software development is an iterative process. Until the Crypto.com Chain stabilizes, Crypto.com will remain being able to upgrade the network directly, taking community contributions into account
by rigorously reviewing pull requests.

Every transaction and every request will include fields related to software versioning.

When a non-backwards-compatible upgrade happens, each honest node will be aware of both the version number and the time the version upgrade should begin, and will thus drop any request or transaction that is broadcasted using an older version.

When two nodes connect, a handshake procedure must be established with remote attestation and some standard checks.
Connected nodes would also periodically check the handshake information with each other; if a connected node is deemed outdated for more than 7 days, it will then be disconnected.

Augmented Decentralization

In line with DA_3, the capabilities of Crypto.com Chain Council Nodes will be split and the entities operating them will be extended to third parties. Adding new Council Nodes (or removing them) requires the approval of at least 67% of all the Council Nodes.

As these proposals for Council Node set changes require an inspection and decisions of Council Node administrators, each proposal will have a set deadline. If a Council Node does not signal a decision after the deadline, it will lose a part of its collateral stake.

This mechanism will enable phased decentralization, meaning that third parties can participate as Council Nodes and ensure that the CRO Network can continue to operate regardless of any unforeseen circumstances in the operation of Council Nodes. Regardless of Council Node-operating entities being removed or added, the transfer of value will still continue to function, and customers and merchants alike can still use the network to spend and receive their cryptocurrencies.

As the large scale distributed consensus algorithms and incentive mechanisms mature, the validation capability may be extended to all nodes that post CRO collaterals.

7. Contribution & Integration

Contribution

Crypto.com Chain code is open source and is available at: https://github.com/crypto-com/chain
We encourage research and peer reviews;
we also support our and external open source projects here through bounties: https://www.bountysource.com/teams/cryptocom
The community can report bugs or request features by opening relevant issues. Any contributor can also suggest bug-fixes or additional features by submitting pull requests. The contribution guidelines are described here:
https://github.com/crypto-com/chain/blob/master/CONTRIBUTING.md
The core development team will review and merge these pull requests according to the contribution guidelines.

Integration: Off-the-Shelf SDKs

Ease of use and integration drive adoption; hence, we will provide acquirers off-the-shelf SDKs and leverage container technologies during integration, paired with documentation that is easy to comprehend.

8. Conclusion

Crypto.com Chain is a privacy preserving payment network that focused on enabling crypto spending in the real world and thus powering the future of mobile money.

Everyone is free to witness and participate in the network. Actors meeting the adequate staking and compliance requirements can perform validation and settlement activities and get rewarded for it.

We will relentlessly iterate our technical design and implementation until Crypto.com Chain is the best way to pay and be paid in crypto— anywhere, anytime, with any crypto, at little to no cost.