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

{chain,contribute}@crypto.com

March 14, 2019
v0.3.0

Abstract

Blockchain technology and cryptocurrencies are a cryptography and security breakthrough as significant as the internet was in 1990s. The technology is however still at a very nascent stage. To generate mass adoption, it will need to find compelling real-life use cases which can appeal to a larger audience than industry professionals and experts. We believe enabling cryptocurrency spending in the real world will be an adoption catalyst. Current traditional payment institutions and existing blockchains have not been able to provide a secure, scalable and decentralized solution to support cryptocurrency payment.

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 without fees. 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 network do not provide a wide-spread, easy to integrate and fast settlement of cryptocurrency in the real world.

Current payment network infrastructures key limitations:

1. Do not integrate with cryptocurrencies systematically;
2. Do not give access to customers nor merchants to reconcile the numbers in a trustless way;
3. Are vulnerable as being the central point of failure;
4. Are expensive to operate;
5. Give low limits on cryptocurrency spending by default;

Existing blockchain-powered payment networks key limitations:

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 and transition to cryptocurrency. Crypto.com Chain is the best way to pay and be paid in crypto, anywhere, any crypto for free.

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 by 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.
- 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
- integration of new acquirers or customer/merchant seamlessly with low technical barriers, right incentives and strict penalties.

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

- it handles double spend naturally,
- it is easier for reconciliation (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. It is the combination of technological design, incentive mechanism, game theory and governance which together nourish a robust system that also allows continuous innovation. Our initially proposed architecture, hence, may undergo future revisions in response to changes in incentives, governance or any 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 in different layers where each node layer is designed to serve 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.

We summarize different node types, their permissions and responsibilities in the table below:

Node type	Who can run it?	Rights and obligations	Requirements
Council Nodes	Initially, Crypto.com Chain servers. Will split and extend this to 3rd party entities as the network scales, based on minimum staking requirements and tier-based randomised selection	Council Nodes have the below rights and obligations: • Execute settlement • Maintain a whitelist log of Council Node identities; • Maintain a whitelist log of Acquirer Node identities; • Maintain a whitelist log of Settlement Agent Node identities; • Order transactions and reward CRO in a limited supply; • Verify all transactions; • Send/receive transactions; • Read data.	• Post CRO collateral; • Dedicated IP; • Meet infrastructure requirements; • Comply to 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; • Send/receive transactions; • Verify related transactions; • Read data,	• Post CRO collateral; • Dedicated IP, *Each acquirer is advised to run multiple nodes to achieve business continuity.
Settlement Agent Nodes	Anyone who has the capability to settle between CRO and	Settlement Agent Nodes have the below rights and obligations: • Sell CRO for other	• Post CRO collateral.

	currencies deemed stable	currencies deemed stable; • Settle for oneself; • Send/receive transactions; • Verify related transactions; • Read data.	
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 can do heavy-lifting tasks and have a reliable always-online network connection. For that reason and DA_2, capabilities of Community Nodes are different from other node types.

Trusted Execution Environments

In order to address DA_1, DA_2, DA_3, and DA_5, core functionality of Crypto.com Chain Nodes is designed to run in secure enclaves of Trusted Execution Environments (TEEs). TEEs, such as Intel SGX[1], Arm TrustZone[2], or Keystone[3], 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 still needs to follow secure coding practices in order to avoid leaks through memory access patterns etc.

An important feature of TEEs is local and remote attestation. This feature enables nodes or external parties to verify that the code they plan to interact with is indeed the certified Crypto.com Chain code. In case of remote attestation, each node does this step before establishing secure communication channels with other nodes.

[1] https://software.intel.com/en-us/sgx

[2] https://developer.arm.com/technologies/trustzone

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

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[4]-like software for protecting their private keys.
3. **Payment protocol enhancements**: TEEs have gained popularity in blockchain systems research, as they can offer high transaction throughputs with low latencies.
4. **Witnessing external data**: for data from oracles or other blockchain networks, TEEs can be used for attesting data authenticity.

In the light of Foreshadow[5] attack, Crypto.com Chain will not solely rely on TEEs for achieving DA_1 and DA_5 and will consider other measures:

- Double attestation scheme: as employed by Tesseract[6] 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[7][8], a programming language that ensures memory safety and freedom of data races.

Consensus

Council Nodes run a BFT consensus protocol among themselves which resolves the final order of transaction sequences. The initial prototype will utilize the Tendermint Core[9] consensus engine. Tendermint works well for PoS / PoA networks, allows high transaction throughputs and gives instant

---

4 https://play.google.com/store/apps/details?id=com.ledger.wallet.bootstrap&hl=en_US

5 https://foreshadowattack.eu

6 https://eprint.iacr.org/2017/1153.pdf

7 https://github.com/baidu/rust-sgx-sdk#rust-sgx-sdk

8 https://edp.fortanix.com

9 https://tendermint.com

finality within 1 second of the transaction completion, which is well aligned with DA_2. It was chosen as the consensus engine for the Chain prototype for the following, additional reasons:

- **Backed by formal research**[10];
- **Robustly-tested implementation**[11];
- **Track record of adoption**[12], 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.

For a decentralized and robust audit log, we will explore using a skipchain, a shared authenticated data structure proposed in Chainiac[13]. To ensure high availability, the total number of Council Nodes in different locations will have to be greater than a minimum set 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 given grace period will be considered dropping out of the network voluntarily.

Security

Being a public network, security (DA_1) and robustness are critical requirements. Future revisions of Crypto.com Chain design will incorporate a detailed threat model. The main challenges and threats are the following:

[10] https://eprint.iacr.org/2018/574.pdf

[11] http://jepsen.io/analyses/tendermint-0-10-2

[12] https://forum.cosmos.network/t/list-of-projects-in-cosmos-tendermint-ecosystem/243

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

DDoS attack

Any write transaction that happens on the network requires a fee payment (by Acquirer or Community Nodes). DDoS attacks will require fee payment as well. By making DDoS costly, rational hackers should be less incentivised to perform such attacks.

Furthermore, DDoS attacks will be further prevented by the Crypto.com Chain staking requirement. Only nodes that stake certain amounts of CRO can broadcast transactions.

Council Nodes and Acquirer Nodes will not be directly exposed to the public internet, but will be accessed through DMZ-style gateways. DDoS attacks using read operations will be prevented by standard practices, such as rate limiting on the gateways.

Unauthorized access to Acquirer Nodes

Once an attacker has gained access to an Acquirer Node, s/he can only block node's external communication or use its interfaces that interact with its core secure enclave code. An Acquirer Node's private data is sealed in an encrypted enclave.

Supplying fake data or forging transactions would require bypassing remote attestation procedures and stealing private keys of all involved parties which are not stored on that node.

For example, a transaction to withdraw funds would require a collective signature of that node's administrators which could be stored externally in HSMs (plus a signature of at least 67% of the Council Nodes).

Blocking a node's external communication is likely to be detected in the affected node's monitoring systems and result in appropriate actions.

Unauthorized access to Council Nodes

Once an attacker has gained access to a Council Node, besides similar implications as in the case of Acquirer Nodes being compromised, s/he can also try to revoke all honest Council/Acquirer Node identities and add his/her own nodes as Council/Acquirer Nodes.

To prevent this from happening, we designed the Council Nodes to be a multi-signature system: when an Council/Acquirer Node is added/updated/revoked, at least 67% of the Council Nodes have to approve this change. When approved, each change is persisted in a distributed immutable audit log, so that all nodes can verify each change and possibly

take an appropriate action (e.g. contacting the affected node's administrators to double check if that change was legitimate).

Supplying fake data of external sources

Apart from CRO data, attacks can be launched using other currencies through the secondary markets. To resolve the potential broadcast of fake blocks by attackers, block messages have to include a multi-signature by at least 67% of all relevant witness nodes (a combination of Council, Acquirer, and Settlement Agent Nodes).

One other possibility are Eclipse Attacks[14] where all witness nodes connect to malicious peers of an external network. Using previously checkpointed blocks with multiple signatures, known counter-measures, such as randomized peer selection and eviction or detection of network anomalies (and extending confirmation times accordingly), need to be implemented to render such attacks infeasible.

Authentic nodes start to behave badly

In the case authentic (non-hacked) nodes start to behave badly, for example, spamming the network, they incur the risk of having all (or part of) their staked CRO tokens be forfeited and being disconnected. This should discourage authentic nodes from becoming bad actors.

Authentic nodes exit the network

Nodes should be free to enter or exit the network without impacting the rest of the network. Their stake will be in a lock-in period.
Historical transactions of such exited nodes are a part of the blockchain history and have already been safely settled.

If any node exits in between a settlement period, the equivalent amount of CRO tokens (with buffer) for unsettled trades will be deducted from their CRO in escrows.

Collateral/settlement account attack by shift of funds

Collateral accounts where the staked CRO of each node is posted are high risk honey pots.
Council Nodes with multi-signatures could move the funds out of such collateral accounts when a node fails to settle or behave badly.

[14] https://eprint.iacr.org/2015/263.pdf

To make it more robust, these accounts are multi-signature accounts locked by at least 67% of Council Nodes.

Escrows with customer settlement accounts and reverse merchant settlement accounts (for refunds) where transient settlement funds sit until the next settlement is done are low risk honey pots.
A multi-signature implementation locked by at least 67% of Council Nodes will be implemented for any cryptocurrency that supports multi-signature. An attacker has to hack 67% of the Council Nodes to be able to shift the funds out.

Front running and other market manipulation attacks
Since communication among nodes is encrypted and data inside nodes are not accessible (as it is sealed in a secure enclave), an attacker cannot exploit much information for executing trades.

One can possible hijack a node, use its CRO collateral and do transactions against non-CRO currencies that can be easily manipulated on secondary markets for a time sufficient for cashing out in products and services of merchants. To alleviate such issues:

1. A transaction time-lock is imposed on CRO collaterals before they can be spent; and
2. A rigorous KYC process and onboarding process is required for all acquirer and council nodes with high responsibilities on the network.

Privacy

As TEEs are used, 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[15] for threshold multisignatures which provide a good tradeoff between privacy and accountability. We will potentially explore employing other techniques, such as additively homomorphic commitments (as used, for example, in Confidential Transactions[16]), where data remains private even in case of

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

secure enclave breaches and its processed parts can be securely and verifiably exposed for third-party auditing.

Compliance

Onboarding of Customer and Merchant Acquirers

Customer Acquirers and Merchant Acquirers are onboarded only if they are able to pass Crypto.com KYC check[17] and comply with KYC standards when they onboard downstream customers and/or merchants.

As mentioned in the Consensus section, CRO may utilize a Chainiac[18]-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 through linking their existing X.509 certificates.

The associated private keys can be securely stored in 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.

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

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

4. Settlement & Price Stability

Routed & Direct Settlement

Routed Settlement

For transactions happening 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, with 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 with 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 concerns them. This way, customers and merchants do 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 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 that transaction.

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. Post 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, but you will have the ability to convert on the spot to currencies deemed stable (inc. stable coins, fiat currencies). Settlement Agents (detailed below) will perform the conversion for merchants and hedge their risk. Settlement time is expected to be around T for crypto conversion, T+2 for fiat conversion.

Settlement Process

Each Acquirer, Community[19] or Settlement Agent Node[20] can maintain their balances by processing blocks which include transactions relevant to them. Transaction relevance can be checked using a fixed-sized probabilistic filter that tags each block.
Without any 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 with 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, or any nodes (whose linked entity) that has a direct relationship with a Settlement Agent, keeps 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 an escrow which can release the CRO to Settlement Agent when 2 out of 3 signatures (Settlement

[19] For direct settlements

[20] For with Settlement Agent trades

Agent signature, Merchant Acquirer signature, Escrow Agent signature) are met.

Scenario A:

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

Scenario B:

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

(B4) Settlement Agent provides a proof to the involved Escrow Agent that the fiat transfer happened.

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

Scenario C: If Settlement Agent fails to send fiat to 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 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 it.

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

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 with 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[21] 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, i.e. [s]% of the CRO token converted. Settlement Agents will be charged by the network a levy and a portion of this levy will be used to reward network participants and ensure long-term sustainability of the protocol.

5. Block Structure & Incentives

The details described in this section, as 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. Exact details, handling etc. depend on interactions with the underlying consensus layer, privacy and security mechanisms.

[21] Benchmark will be likely calculated using a verified external price source collected using an oracle.

Data Structure

Transaction Data Structure

The accounting model in the initial prototype of Crypto.com Chain 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 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.

Depending on the implementation, it may additionally include references to past data needed to be fetched for transaction validation.

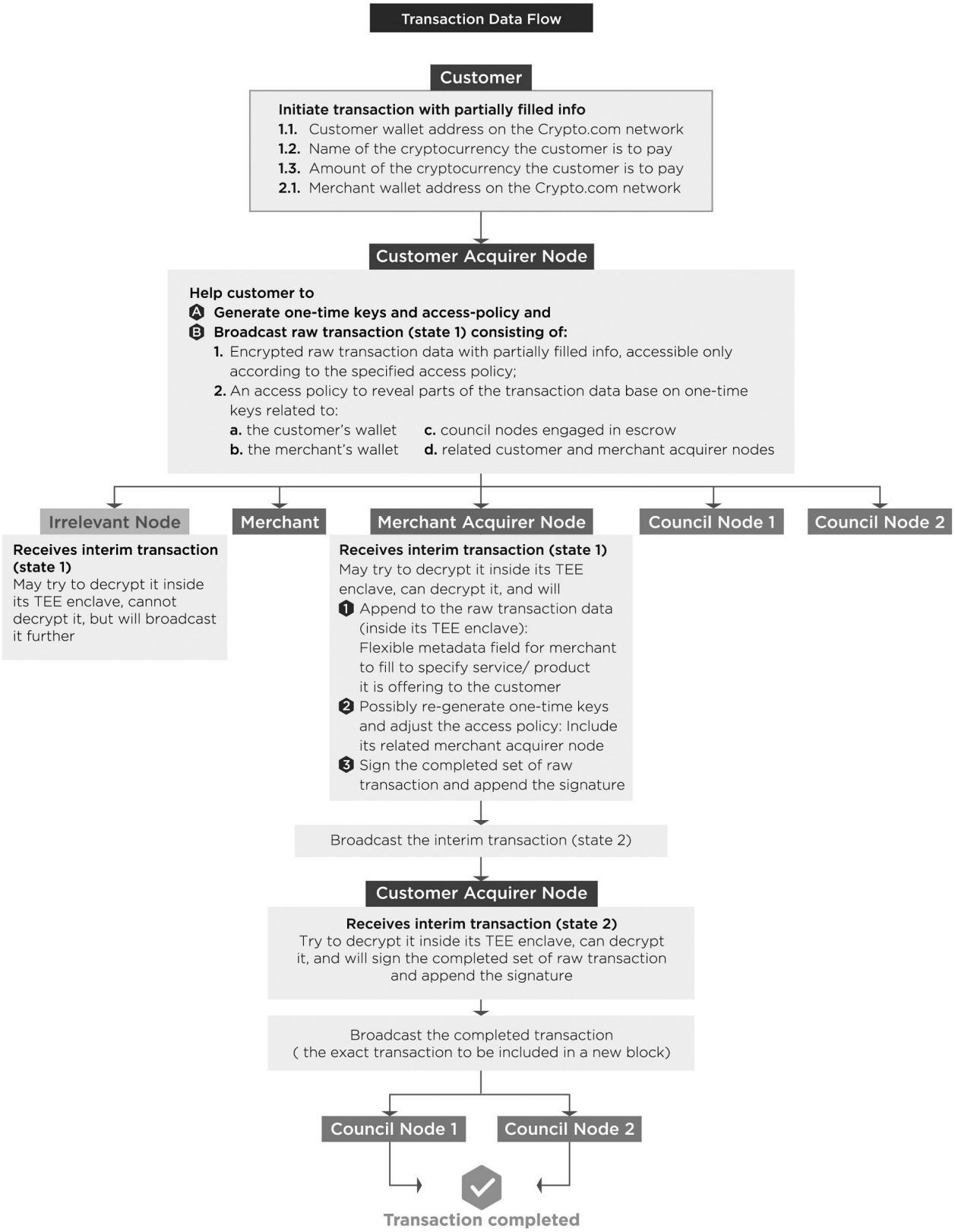
Part A) Raw transaction data will never be revealed directly, as discussed in Privacy. The following encrypted data may contain additional obfuscation to prevent data leaks in case of TEE access policy breaches:

1. Transaction data:
    a. Transaction inputs
    b. Transaction outputs
2. An access policy of what can be exposed to whom 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: versioning information, network identifier, metadata related to the use of external currencies.
4. Collective witnesses, 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. By doing so, this will help to ensure the ease and consistency of implementations across different programming languages used in third party integrations.

Transaction Data Flow Summary:



Block Data Structure

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

https://tendermint.com/docs/spec/blockchain/blockchain.html#data-structures

Crypto.com Chain will employ these additional conventions:

1. AppHash will be a root of an authenticated data structure, such as a Merkle tree, constructed after committing a set of valid transaction in a given block. Given AppHash, 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, 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. They 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.

Transaction Rewards

In both routed or direct settlement scenario, the merchant and customer can use the Crypto.com Chain for free.

The Crypto.com Chain distributes *[x]* rewards to all actors providing services to ensure integrity and successful processing of the transaction.

[x] is calculated based on:

- CRO daily distribution supply, and,
- levy collected from Settlement Agents.

[x] is allocated to participants based on:

- transaction amount processed by Acquirers, and,
- number of transactions validated by Council Nodes

$$[x] = [c_{\%}] + [m_{\%}] + [p]$$

- $[c_{\%}]$ goes to customer acquirer for service rendered,
- $[m_{\%}]$ goes to the merchant acquirer for service rendered,
- $[p]$ goes to the Council Nodes for service rendered,

In a direct settlement scenario,

- $[c_{\%}] = 0$
- $[m_{\%}] = 0$

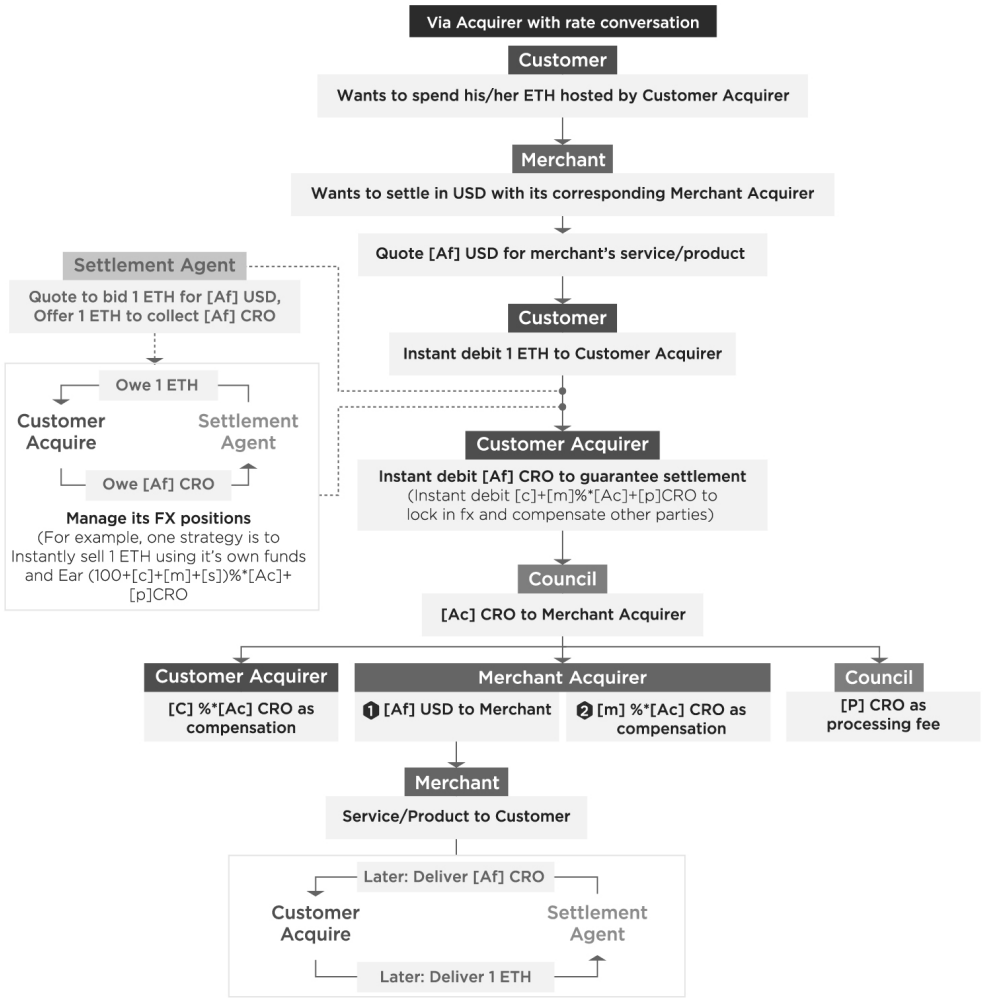
The Crypto.com Chain also requires a transaction fee $[y]$ for any write transaction sent by network participants. This transaction fee is added to their stake immediately and given back to the participant at a later stage.

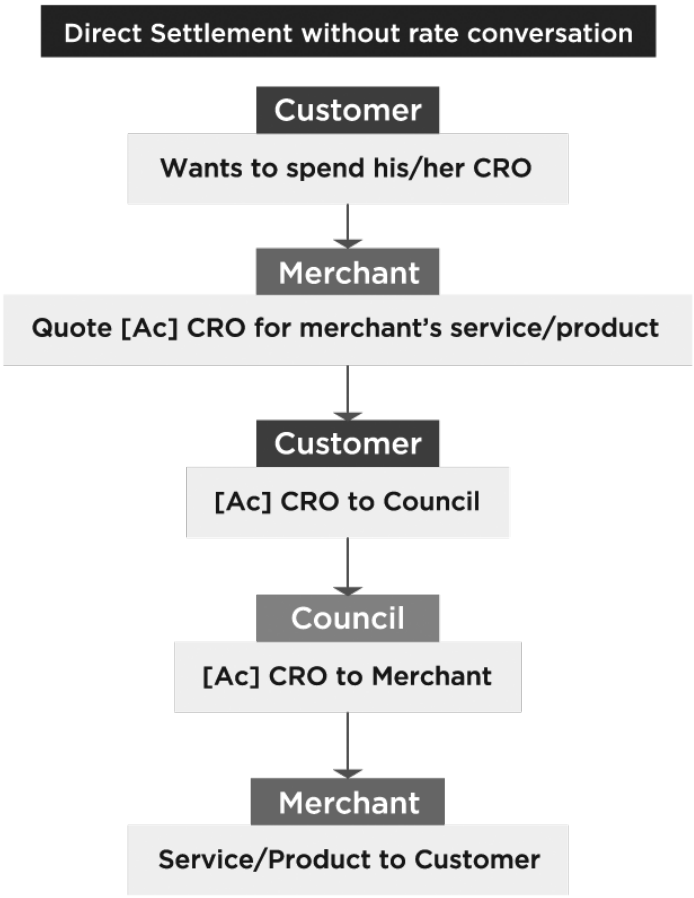
The Crypto.com Chain will extract rewards from the Secondary Distribution & Launch Incentives Pool and subsequently the Network Long Term Incentive Pool.[22]

For preliminary views on Crypto.com Chain staking mechanism, please refer to the Consultation Paper.

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

Summary diagram:




Direct Settlement without rate conversation
Customer
Wants to spend his/her CRO
Merchant
Quote [Ac] CRO for merchant's service/product
Customer
[Ac] CRO to Council
Council
[Ac] CRO to Merchant
Merchant
Service/Product to Customer

Dispute Resolution

Refund

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

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

Double spending

The consensus algorithm and cryptographic measures are set up, such 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 robustness of the network, a minimum number of Council Nodes spread across the globe will need to be up and running. The minimum number is to be decided based on real performance test to balance 1. robustness against compromising a supermajority of Council Nodes; and 2. efficiency/high-performance.

Network Scalability & Performance

Crypto.com Chain targets 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 explore other advances in the field such as 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[23]. The Schnorr signature scheme has been recently proposed for the Bitcoin network[24]. One of its most compelling applications are compact multi-signatures where n-of-n signatures are no different from ordinary signatures from the verifier's perspective.

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

One such development direction is in blockchain compression approaches. For instance, Coda[25] is a proposed cryptocurrency protocol which 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. It does so through recursive composition of zk-SNARKs. Coda promises to reduce the enormous blockchain sizes from hundreds of GBs or TBs to a few KBs.

When bootstrapping procedures are developed for Tendermint Core, Crypto.com Chain may allow safe snapshotting and pruning 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[26] 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.

Upgrading the Network

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

---

[23] 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

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

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

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

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

When a non-backwards-compatible upgrade happens, each honest node would know the version number and the time the version upgrade must start and will drop any request or transaction that is broadcasted with an older version.

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

Augmented Decentralization

In line with $DA_{\mathscr{J}}$, 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 an approval of at least 67% of all the Council Nodes.

As these proposals for Council Node set changes require an inspection and decision by 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 where 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 would still be functioning and customers and merchants could 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 posted 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. One 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 easy to comprehend documentation.

8. Conclusion

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

Everyone is free to witness and participate in the network. Actors with 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, any crypto, for free.