A New Distributed and Decentralized Internet

Technology Whitepaper

1. Overview

The internet is the world's shared network where we communicate, learn, and work. For much of the world, a life without internet access would be unimaginable. For the rest of the world, a connection and access to the internet transforms lives. But much of the internet we use today was designed and developed a couple decades ago. As the rest of technology matured at faster and faster speeds, our shared internet became more vulnerable and many problems were visible. We have faced major cyberattacks and hacks on centralized services and debate on the centralized ownership of data. It's time for the internet to be updated.

The Chromata protocol is a new, open-source and decentralized take on the internet with the goal of making our world's shared network faster, safer, and freer for everyone. Chromata consists of five components:

1. Decentralized Network: A peer-to-peer communication protocol that uses a hypertext application protocol based-on content addressing, a decentralized overlay network, and encryption to make our internet faster and safer.
2. Decentralized Name System: A decentralized name system to map human-readable names with a unique address while eliminating centralized points of failure and returning ownership of data and identity to the user.
3. Decentralized Compute Platform: A smart contract-based computing platform to run decentralized applications accessible by a client application browser that are unstoppable and safe from censorship, fraud, and unavailability.
4. Decentralized Storage: A blockchain-based immutable, decentralized filesystem for the storing of static content and the storage of dynamic data in the blockchain to be accessed through applications to make the internet distributed, resilient, and open.
5. Decentralized Economy: A decentralized economy built on top of the Chromata network powered by a stable currency that is the basis for the network's transactions and various free markets to enable a free exchange of data, goods, and ideas.

These five components allow for decentralized applications to run on the Chromata network and be accessed by anyone with a client application browser. The Chromata protocol layers can be seen below in Figure 1.

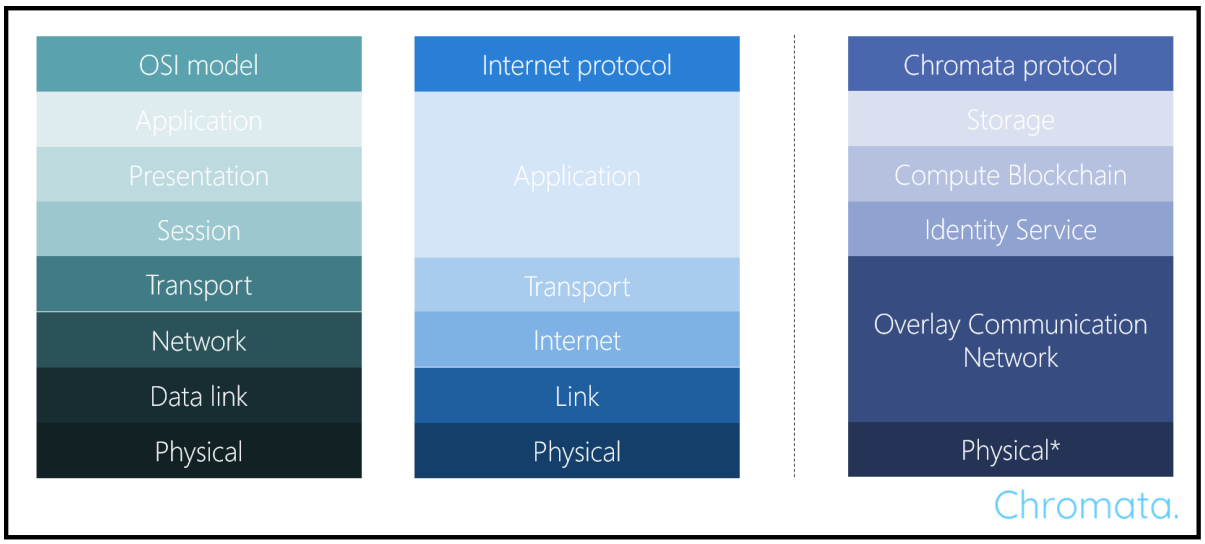

Figure 1: A comparison of the layers of the OSI model and the Internet protocol with the layers of the Chromata protocol. The Internet model's Application layer is split among Layers 1 through 3 in the Chromata protocol, each of which is detailed in this whitepaper. Layers 2 through 4 of the Internet model correspond to the Overlay Communication Network Layer in the Chromata model and this is also detailed in the whitepaper. Layer 7 (the layer with the *, Physical) of the Chromata protocol will be detailed in another whitepaper. The Economy layer of the Chromata protocol sits above the application layer so is not shown here but is detailed in the whitepaper.

The Chromata protocol uses the existing Physical layer and infrastructure of the Internet model but is compatible with other Physical infrastructure as it is deployed. The Chromata protocol also uses the existing Transport layer of the Internet model such as TCP (Transmission Control Protocol) and UDP (User Datagram Protocol) but uses an overlay network and a new communication protocol on top of the existing Transport layer.

This whitepaper covers the core blockchain technology that is the base framework that the rest of the Chromata protocol is built on top of. A separate whitepaper will cover the decentralized compute, storage, and bandwith markets as well as the decentralized name system and a decentralized exchange. Another whitepaper will also cover the business aspects as well as a roadmap for the development of the Chromata protocol technology and the ecosystem.

2. Blockchain Network Architecture

The Chromata protocol uses a network of blockchains for the Compute, Identity, and Communication layers as well as a part of the Storage layer. The Chromata protocol consists of a network of independent blockchains that are all connected to a single public mainchain and can be connected to private, permissioned sidechains. In the Chromata network the public mainchain has application-specific smart contracts for public decentralized applications and the private, permissioned sidechains are for

application-specific smart contracts for private decentralized applications. Each independent blockchain is powered by a simple Proof of Work algorithm, represents a single individual, and can only be updated by the individual it represents. These independent blockchains are made up of transaction blocks and make up state channels with other independent blockchains allowing for the mainchain to act as a public state machine and the sidechains to act as private state machines for private decentralized applications. The public mainchain can be accessed by any client on the Chromata network while each private, permissioned sidechain is created by a business, consortium, or other organization and its access and consensus is controlled by a specific authority as part of the Proof of Authority algorithm used on these blockchains.

I. Clients, Nodes, and Accounts

Individuals on the Chromata network have their own independent blockchain and key pair with a public key and private key. This independent blockchain is the source for all their actions within the Chromata network and can be accessed by multiple wallets. To be able to update the independent blockchain, the entity needs the key pair that represents their identity and each transaction is signed by the private key of the sender. In cases where a transaction is between two or more entities, the public keys are used as destinations to receive the transaction. Each identity on the Chromata network can also have multiple credentials, each used for a different decentralized application. For example, a single identity could have the necessary credentials for multiple different public and private decentralized applications. Credentials are issued when an entity uses a SEND transaction to send the corresponding credential asset to an identity. Credentials are used when an entity requests the credential with the necessary data in a RECEIVE transaction. This can be for authentication into a decentralized application, KYC, or for many other uses. Once a credential is issued, it is reusable by the entity to which the credential is issued. Credentials can be defined as permanent, these are owned by the entity to which the credential is issued such as a credential used for authentication into certain applications, or temporary, these are credentials for which certain rules are set for ownership of such a credential. An example of a credential that is temporary would be citizenship to a certain jurisdiction which can be acquired through naturalization and given up through renunciation or a certain accreditation such as a credit score which can change over time. Entities such as connected or IoT devices, artificial intelligence, and other machine-based entities also use this identity system with their own individual blockchains. Smart contracts, on the other hand, do not have their own individual blockchains but rather run on the mainchain. They do have public-private key pairs like the other entities and can be issued credentials as well.

II. Transactions

In the Chromata network only two types of transactions can occur: SEND and RECEIVE. All transactions sent from an independent blockchain must have a transaction type, be signed by the corresponding entity's private key, have a specific application represented by the application id, have a reference to the work from the Proof of Work algorithm, a reference to the hash (this hash uses SHA-3) of the previous block in the independent blockchain, have information on any header fields necessary like status, and have information on any other fields (body content) required by the specific application as shown in Figure 2. These transactions are broadcast to the mainchain or sidechain of the respective application through the application-specific smart contract that uses the transaction data to update the application-specific database. In transactions where the recipient of the asset is an application, there is no need for a RECEIVE transaction as the application-specific smart contract handles the distribution of the assets to the application-specific database. The RECEIVE transaction can be used however for an individual to receive information they have access to from an application-specific database. RECEIVE transactions are also used when an asset is transacted between two or more entities where the sender(s) use SEND transactions to send the assets and update the application-specific and the receiver(s) use RECEIVE transactions to receive the assets.

```
transaction {
      transaction type:
      private key:
      applicationid:
      work:
      previoushash:
      headerfields:
      bodycontent:
}
```

Figure 2: A sample transaction where the transaction type would be SEND or RECEIVE. A sample field for a cryptocurrency application could be a transaction destination (or the public key of the recipient for a send transaction).

III. Assets

All forms of data on the Chromata network are assets whether that be cryptocurrency information or a string of text. These assets are always a part of a

specific application and in the case of cryptocurrencies or other financial assets among other use cases the asset and application can have the same name (for example the CMT cryptocurrency's asset and application have the same name but the CMT application also encompasses other assets such as balance information). These assets can be sent, received, or accessed through the transactions and a smart contract connected to each application's database stored on the Chromata mainchain or a private sidechain. The database can be structured to hold any type of information in the form of assets and will be immutable and will use a Byzantine fault-tolerant Proof of Stake (for the mainchain) algorithm to reach consensus when a conflict arises. This works where an entity creates a SEND transaction for a specific application and this sends the information contained in the transaction block on the entity's individual blockchain to the application's specific smart contract. Each smart contract is developed to perform an application-specific action where the application's database receives a new entry and a certain action is performed as shown in Figure 3.

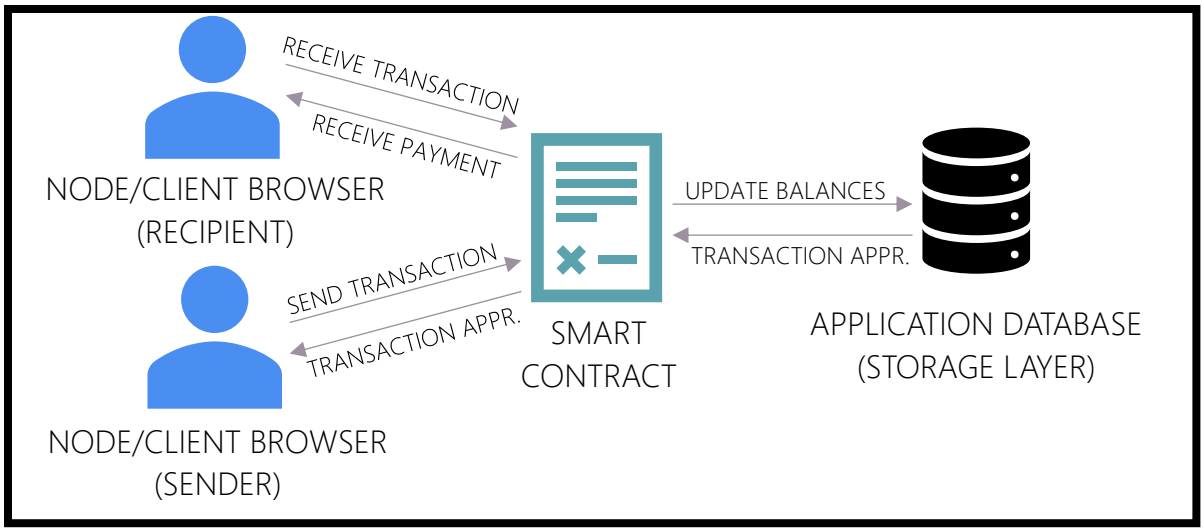

Figure 3: A sample cryptocurrency transaction being broadcast to the network where an independent blockchain would create a SEND transaction with a recipient and the smart contract would process the SEND transaction, update the database on the mainchain with the sender's new account balance, and wait for a RECEIVE transaction from the specified recipient. When the RECEIVE transaction is broadcast to the smart contract, update the database on the mainchain with the recipient's new account balance, and the transaction would be complete.

IV. State Channels

By default, all transactions and applications using the Chromata network use asset-specific state channels. Transactions occur off of the mainchain/sidechain and on individual blockchains but update the smart contracts' state for the respective application on the public mainchain or private sidechains. This allows the Chromata blockchain network to scale with bandwith limits as the use of a consensus algorithm and validator set is not necessary for every block or transaction to be confirmed.

Instead, the Byzantine fault-tolerant Proof of Stake is only needed when a fork occurs due to malicious intent or an innocent error much like a court or arbiter is only needed when a dispute occurs. When a dispute does occur, the Byzantine fault-tolerant Proof of Stake decides which child block to continue with and the dispute is resolved.

V. Smart Contracts

All applications in the Chromata network run using smart contracts which run on the mainchain in the case of public decentralized applications and on private sidechains in the case of private decentralized applications. The mainchain acts as a public state machine for application and by default keeps the latest state of smart contracts actively running on the blockchain. Private sidechains act as private state machines but also keep track of the latest state of smart contracts that power the private decentralized applications running on the respective sidechain. Smart contracts are self-executing and can be event or transaction-driven. The smart contract code is pre-written and cannot be changed making smart contracts immutable. Data on the latest state of the application in an internal ledger in the smart contract and can only be updated by SEND transactions with a destination at the respective smart contracts. RECEIVE transactions can be used to retrieve data from the smart contract with the necessary credentials. Smart contracts can also have a pre-programmed status which can be active, pending, or completed. This is used when a smart contract is temporary such as an agreement between two or more parties.

VI. Mainchain Consensus

The mainchain is the blockchain to which all individual blockchains and sidechains connect to in the Chromata network. When a fork occurs on an independent blockchain via malicious intent or an innocent error, the mainchain must only connect to a single independent chain (regarding each entity's individual blockchain) so to decide on which child block to connect to, the Byzantine fault-tolerant Proof of Stake algorithm is used. This vote on the fork in an individual blockchain is commenced when a validator alerts the network to a fork on an independent blockchain with the block whose hash is referenced as the previous hash into child blocks and the Byzantine fault-tolerant Proof of Stake algorithm begins. The algorithm works by having a set of validators that vote on which child block to use in voting rounds and each of the validators has a collateral (denominated in CMT) that can increase with rewards and decrease with penalties. A penalty is given out when a validator broadcasts two conflicting votes for the same open voting round. Rewards are paid out when validators accurately bet on what other validators will bet. This

system leads to a convergence in the bets of validators. Each validator's vote is equivalent to their collateral and for a child block to be chosen it must receive greater than 2/3 of the total collateral in the form of validator's votes. When a certain child block is chosen the other is disregarded as false and a single independent blockchain continues. The validator who initially alerted the network to the fork is paid a reward after the process is completed.

VII. Sidechains

Sidechains are private, permissioned blockchains independent of but connected to the public mainchain and individual blockchains. Sidechains are created by a specific company, organization, consortium, or other entity and has a Proof of Authority consensus algorithm run by validators set by the sidechain's creator. The validators also decide which entities can access the private sidechain and can manage roles and capabilities for each entity as well. Private decentralized applications running on private sidechains cannot be accessed by the public or anyone without the necessary credentials (issued via a SEND transaction from the validators in that private sidechain's Proof of Authority algorithm). Sidechains have all of the same capabilities as the public mainchain including issuing cryptoassets and creating smart contract-based decentralized applications among others but with the private, permissioned nature of the Proof of Authority algorithm.

VIII. CMT (Stable Cryptocurrency)

The Chromata token (CMT) will be the cryptocurrency that will power the economy built on top of the Chromata blockchain and is the currency used in the Byzantine fault-tolerant Proof of Stake consensus system. The Chromata token is relatively stable in value through a smart contract-based mechanism detailed below and will be used for utility on top of the blockchain as opposed to as a form of investment (investment-focused digital assets are a separate type of financial asset in the Chromata economy). The Chromata token is a fungible asset that can be integrated into decentralized applications and other solutions on top of the blockchain. The CMT token will be regulated using a set of smart contracts that trade on the open market to expand or contract the money supply which will allow for price stability and will work by using a two-part system of the currency itself and a reserve asset, CMT.R. Initially the value of the CMT token will be pegged to the value of the International Monetary Fund's (IMF) Special Drawing Right (SDR), an international reserve basket of the US dollar, the euro, the British pound sterling, the Japanese yen, and the Chinese renminbi. But when the CMT token-powered economy reaches a self-sustaining size the CMT token can be switched from being pegged to the SDR

to being pegged to a basket of consumer goods within the Chromata economy. This would allow for the CMT token to account for inflation and deflation in the economy as opposed to just price stability of the token. The smart contracts expand the money supply when the value of CMT is increasing against the peg by paying CMT.R holders new CMT tokens as a dividend creating a downward pressure on the value of CMT due to an increase in supply and can contract the money supply when the value of the CMT is decreasing against the peg by selling new CMT.R to the public to create an upward pressure by decreasing the supply as shown in Figure 4. CMT.R can be bought and sold at any times on an exchange just like the CMT cryptocurrency itself but will be a volatile asset unlike CMT. This smart-contract based acts as a coded monetary policy for the CMT asset.

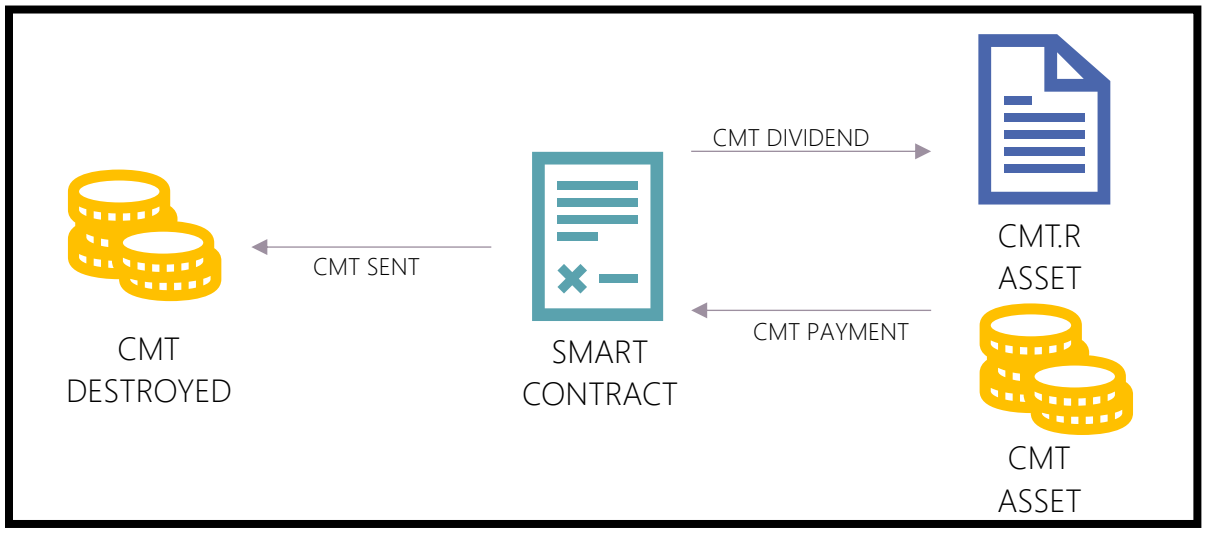

Figure 4: When the CMT price is decreasing, the smart contract can contract the money supply by selling CMT.R to the public. When CMT is paid to acquire the new CMT.R, the CMT is destroyed by the smart contract and the CMT.R is distributed. The CMT.R gives it holders the right to dividends paid out when the smart contract decides the money supply must be expanded.

3. Attacks

Double Spending – A double spend occurs when two transaction blocks referring to the hash of a single previous transaction block in an independent blockchain. This is called a double spend as in the case of cryptocurrency, this would cause the same cryptocurrency to be spent twice. When these two conflicting transactions are broadcast to the mainchain through malicious intent or an innocent error on the independent blockchain's owner's part, a fork occurs. The built-in Byzantine fault-tolerant Proof of Stake mechanism on the mainchain handles deciding which independent chain, on the individual blockchain, the mainchain must connect to. Because the validator set described above must be able to change over time, existing validators can leave the validator set and new validators can join. New validators can join by creating a SEND transaction to the validator set smart contract with their

collateral and existing validators can create RECEIVE transactions to bring their collateral back under their control. Once a validator leaves the validator set, their public key cannot join again.

51% Attack – A 51% attack when an entity with enough stake in the system to form a majority can compromise the network. On the Chromata network, this form of an attack would take more than 2/3 of the network to collude as a 2/3 majority is required to cause a change in the network. Because the Byzantine fault-tolerant Proof of Stake system uses votes in proportion to the total collateral, a 51% attack on the Chromata network would also be very expensive as it requires a single entity or a group of colluding entities to acquire over 2/3 of the total collateral to perpetrate a 51% attack. A network Denial of Service attack could be used to decrease the value of the total collateral and hence the amount needed for the 51% attack to be perpetrated, though. But because the validator set and collateral database itself resides as part of the Chromata mainchain, in the case that the 51% attack with the purpose of breaking the network succeeds, and the network is compromised, the collateral of the attacker(s) would also be lost. This makes this kind of an attack even more expensive for the attacker(s).

Long-Range Revision Attack – A long-range revision occurs when a group of validators that once represented 2/3 of the total collateral withdraw their deposit and exit the validator set but then use their historical 2/3 majority to change the result of disputes solved by the Byzantine fault-tolerant Proof of Stake consensus algorithm. This attack would not work on the Chromata blockchain network as blocks that have been added to the mainchain in the past cannot be reversed after their respective smart contract's state has been updated. As long as an entity has seen the updated state for the respective smart contract, a long-range revision will simply be ignored by that entity and activity based on the smart contract's most recent state can be continued.

Sybil Attack – A Sybil attack, in which an entity floods a network with multiple new nodes to gain control of the network, would not work on the Chromata network as consensus is not based on the number of nodes but rather the collateral posted by each validator in the set and their votes. As a result, the combined voting power of a thousand nodes with the same combined collateral as one node would be the same as the one node.

Catastrophic Crashes/Network Partition Attack – A catastrophic crash attack, in which more than 1/3 of the total collateral in the validator set simultaneously go offline due to malicious attack or a computer failure or where validators refuse to participate in the consensus process, would not cause a problem in the Chromata

network as validators are penalized for not participating in the consensus process. To avoid this, validators that do not want to participate in the consensus process can withdraw their deposit and exit the validator set or can have the amount taken from them as a penalty for inactivity returned after a certain period of activity. This inactivity penalty also works to decrease the total collateral such that the collateral that is still active can make up a 2/3 majority again.