MultiChain helps organizations to build and deploy blockchain applications with speed.

Rapid deployment

Just two simple steps to create a new blockchain, and three to connect to an existing one. Deploy unlimited blockchains per server for cross-chain applications.

Unlimited assets

Issue millions of assets and tokens, all tracked and verified at the network level. Perform safe multi-asset and multi-party atomic exchange transactions.

Data streams

Create multiple key-value, time series or identity databases. Store data on- or off-chain. Ideal for data sharing, timestamping and encrypted archiving.

Fine-grained permissions

Optionally control who can connect, send and receive transactions, create assets, streams and blocks. Each blockchain is as open or as closed as you need.

Developer friendly

Designed to let developers build blockchains and applications with minimum hassle.

Customizable

Full control over every aspect of the blockchain, proof-of-work is optional.

Flexible security

Supports multisignatures, external private keys, cold nodes and admin by consensus.

- MultiChain is an extended open source fork of Bitcoin.
- It can be used to launch custom blockchains, both private and public and is easy to configure.
- It offers a well-selected set of features and enhancements targeted at enterprise and business users.
- The support for native assets and storage of larger amounts of arbitrary data seems promising.
- An optional but unique approach is taken with the consensus based permissions management for consortial blockchains.
- In the context of a public blockchain these features are less interesting. All these extensions are achieved while maintaining compatibility to

many technical aspects of Bitcoin Core; hence, much of the Bitcoin documentation is applicable to MultiChain as well. This compatibility makes MultiChain a promising candidate, because most Bitcoin-compatible approaches will apply to MultiChain too.

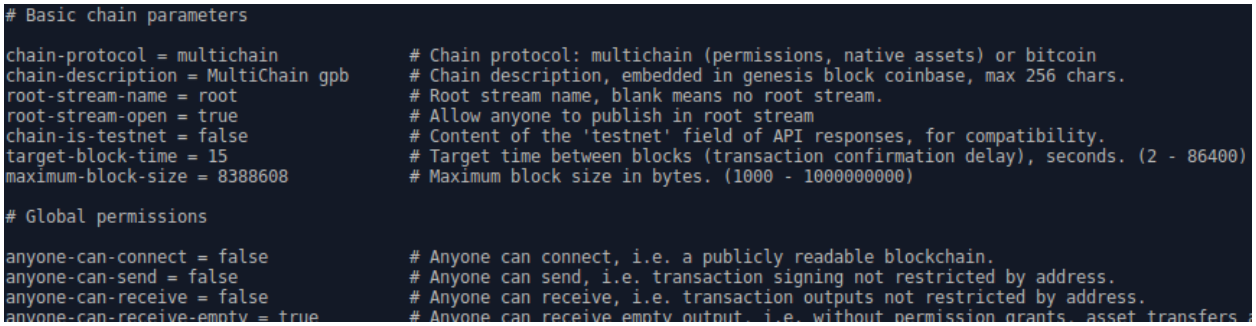
- Additionally, “flexible creation and transaction of custom assets/tokens” is of particular interest for us and natively supported by MultiChain.
- It is also noteworthy that the project is developed in a very transparent way: questions posted to the official Q&A-section are answered quickly and competently.
- Since MultiChain expects users to create their own blockchains for their specific use cases, there is no “official” public blockchain network which could have proven its stability and security. However, being a fork of the bitcoin code base, its fundamentals should be sound and it is very simple to setup a local chain for testing.

SETUP

A typical MultiChain installation is made up of three executables:

- *multichain-util* is used exactly once to initialize a new blockchain
- *multichaind* runs a node to host the chain
- *multichain-cli* is the client to perform actions on the chain

The chain is customized by editing a simple text file generated by *multichain-util*; this must be done before running *multichaind* for the first time because settings cannot be changed once the chain has been fully created.



```
# Basic chain parameters

chain-protocol = multichain             # Chain protocol: multichain (permissions, native assets) or bitcoin
chain-description = MultiChain gpb      # Chain description, embedded in genesis block coinbase, max 256 chars.
root-stream-name = root                 # Root stream name, blank means no root stream.
root-stream-open = true                 # Allow anyone to publish in root stream
chain-is-testnet = false                # Content of the 'testnet' field of API responses, for compatibility.
target-block-time = 15                  # Target time between blocks (transaction confirmation delay), seconds. (2 - 86400)
maximum-block-size = 8388608            # Maximum block size in bytes. (1000 - 1000000000)

# Global permissions

anyone-can-connect = false              # Anyone can connect, i.e. a publicly readable blockchain.
anyone-can-send = false                 # Anyone can send, i.e. transaction signing not restricted by address.
anyone-can-receive = false              # Anyone can receive, i.e. transaction outputs not restricted by address.
anyone-can-receive-empty = true         # Anyone can receive empty output, i.e. without permission grants, asset transfers
```

Excerpt of the generated configuration file. All parameters are well explained in addition to their online documentation. Crucial settings, like the block-time, required permissions and mining constraints are easily changed to accommodate the application's needs.

Applications of Multichain

FEDERATED MANAGEMENT OF CONTENT IDENTIFIERS AND METADATA

Streams on MultiChain are publicly readable, append-only key-value databases on the blockchain whose items can reach "many megabytes in size". Being append-only, an application can still extract older, "good" data from the stream if some user attempted to overwrite it maliciously. Despite being public, there are ways to store confidential data in a stream but they are a bit cumbersome to implement. A total stream size of multiple gigabytes is possible and the announced transaction rate of 500 tx/sec for insertion-transactions seems promising. By design, these numbers will only hold true in closed setups that do not depend on proof of work and use a permissions based round-robin consensus instead.

FLEXIBLE CREATION AND TRANSACTION OF CUSTOM ASSETS/TOKENS

MultiChain allows the dynamic creation of native assets by anyone with appropriate permissions. These assets can be traded directly on the chain so that all nodes validate such transactions in the same way they would validate the chain's native currency. Additionally, MultiChain allows atomic exchanges of arbitrary assets (including the default currency), so that different assets, whether they represent licenses, ratings or actual monetary value, can be safely and efficiently traded on the chain.

SUPPORT FOR CUSTOM BLOCKCHAIN APPLICATION DEVELOPMENT (SMART CONTRACTS)

MultiChain does currently not support the on-chain execution of Turing complete smart contracts like for example Ethereum does. However, smart contracts are a much discussed topic [1, 2] and the MultiChain developers have not ruled out smart contracts completely, but they want to see "strong use cases" [3] which cannot be solved using a combination of multisignature transactions, client side logic and trusted third parties.

REMARKS

During testing one thing became clear quite soon: Decentralized consensus based permissions management (if used at all) becomes a liability and a management challenge very fast. The fact that the percentage of administrators needed to approve changes is set in stone at the launch time of the chain would make it hard to accommodate for a growing community. While it is convenient that MultiChain is completely agnostic to what data is posted or stored in streams or metadata it also opens the door to spam streams with data that is invalid in the context of their intended use. A mechanism to bind validation of transaction data against a given schema to the consensus system would be helpful.

RESULT

The possibility to use MultiChain as a public, large and distributed data storage makes it a promising candidate for the ISCC (International sustainability and carbon certification: **ISCC certificates as issued by the certification body are valid for their indicated validity period even if they are not yet published on this website**. ISCC lists the certificate information in the table below after receiving the relevant documentation from the certification body. The respective pdf files of the certificate and the summary audit report are published once the ISCC internal document review has been completed. Scope adjustments that took place during a recertification will be updated in the table during the ISCC internal document review.

Expired certificates are marked red. The number of certificates is crossed out, if a certificate was withdrawn.A certification according to the waste and residue process does not mean that EU Member States automatically accept the material as waste or residue) database. In combination with tradable custom assets, conventional license trading, that is handing over a signed legal paper to a purchaser, could be moved onto this digital platform. The biggest remaining issue seems to be a sensible mining configuration to ensure the chain's resistance against spam, censorship and centralization.

Source: https://content-blockchain.org/research/multichain/

Permissions in multichain :

Source:
https://www.multichain.com/developers/permissions-management/#:~:text=Permissions%20in%20MultiChain,in%20the%20outputs%20of%20transactions.

Privacy in multichain
Source: https://www.multichain.com/privacy-policy/

MultiChain Privacy Policy

This notice explains how your information is collected and used.

The MultiChain software program ("MultiChain"), which allows users to create, manage and transact on a private blockchain, as well as documentation relating to MultiChain (all of the foregoing, the "Services") through the Site and related subdomains. This Privacy Policy explains how your information is used and collected by the Services and the Site.

Information That is Collected

Personal Information. When contacting us via an online form, we may collect, save or otherwise keep in our possession certain information that identifies you personally or which may be associated directly with you, such as your personal name, company name, company address, email address or website address ("Personal Information"). We may collect such information through your use of the Site and/or Services.

Notwithstanding the above, upon request, we will make good faith efforts to inform you of any Personal Information we have stored, and correct or delete this information as desired. We will ask you to identify yourself and the appropriate information before fulfilling such as a request.

Non-Personal Information. We may also collect, save or otherwise keep in our possession information that does not identify you personally, such as your history of use of the Site and/or Services, IP address and IP address-related information, including the country or state in which you are located, method of connecting to the Internet and other related information, as well as browser information, such as browser name, operating system, version, language and other related information. We refer to information that does not identify you personally as "Non-Personal Information".

By using the Site and/or Services, you voluntary agree to provide us with any information, and to collect, save or otherwise keep in our possession such information (including Personal Information). If you refuse to provide us such information, you may not have access to all functionality of the Site and/or Services.

Please note that while we make reasonable efforts following industry standards to secure all information referred to above, it is impossible to have such information completely secure. As such, we cannot accept any liability for the disclosure of Personal Information as a result of unauthorized access to our Site or MultiChain.

How We Use Information

We will not sell, trade or rent your Personal Information to unaffiliated third parties unless you explicitly provide us with permission to do so. We use Personal Information to help diagnose problems with our servers and/or other parts of the Site, and to make the Services more useful for you and for our other customers. We may also use any information to resolve disputes and to enforce MultiChain's Terms of Service, which are available at http://www.multichain.com/terms-of-service/.

In addition, by analyzing the information we are provided or we collect, save or otherwise keep in our possession, including all Personal Information, we may compile certain statistical information, such as without limitation anonymous information about how users use the Site and/or Services (the "Statistical Information"). We may analyze such information directly or by using third party services, including but not limited to: (a) Google Analytics to track visitor activity on the Site; (b) Digital Ocean for website hosting; and (c) Rackspace Cloud to provide a CDN (content delivery network) for downloading files. Statistical Information helps us understand trends and users' needs so that new products and services can be considered and so existing products and services can be tailored to our users' desires. Statistical Information is anonymous and will not be linked to any Personal Information for provision to third parties. We may share such Statistical Information with our affiliates, without restriction, on commercial terms that we can determine in our sole discretion.

Legal Disclosures. In the event we are required to disclose Personal Information or Non-Personal Information, or any other related information pursuant to lawful requests, such as subpoenas or court orders, or in compliance with applicable laws or regulations, we will make such disclosure. It is our policy to cooperate with law enforcement agencies, and we will fully cooperate with any ongoing law enforcement investigation, including to the extent we are required to disclose Personal Information.

Change of Ownership. In the event the ownership of all or a part of our business were to change, your Personal Information and other related information pertinent to the business' operations would likely be transferred to, or licensed for use by, the new owner.

To Protect Us or You. We may disclose your Personal Information and other related information in the event we reasonably believe such disclosure is necessary to protect the Site or Services, our rights or property, or the rights of any third party. We may disclose your Personal Information and other related information, when we have reason to believe that disclosing such information is necessary to identify, contact or bring legal action against someone who may be violating this Privacy Policy or may be causing injury to or interference with (either intentionally or unintentionally), our rights or property, other users, or anyone else that could be harmed by such activities. You thus authorize us to disclose any information about you to law enforcement or other government officials if we, in our sole and absolute discretion, believe that such disclosure is necessary or appropriate.

Cookies

A cookie is a small piece of text that is sent to a visitor's browser. The browser provides this piece of text to the device of the originating visitor when this visitor returns. A "persistent" cookie may be used to help save your settings and customizations across visits. Most web browsers are initially configured to accept cookies, but you can change this setting so your browser either refuses all cookies or informs you when a cookie is being sent. Also, you are free to delete any existing cookies at any time. Please note that some features of the Site may not function properly when cookies are disabled or removed.

Third Party Sites and Services

We are not responsible for the use of any data by third parties, and we cannot vouch for the privacy policies of any third party. The Site and/or Services may link to or use web sites or services belonging to third parties. We have no control over third-party sites or services, and all use of third-party sites or services is at your own risk. We cannot accept responsibility for the privacy policies of any such sites. We are not responsible for content available by means of such sites or services. We do not endorse any services or offered by third parties and we urge our users to exercise caution in using third-party sites or services. When we provide information to third parties, we remove any information that identifies any particular individual or user, such as a name, address or contact information, but we cannot provide complete assurance that the recipient will not be able to associate such de-identified information with a particular individual.

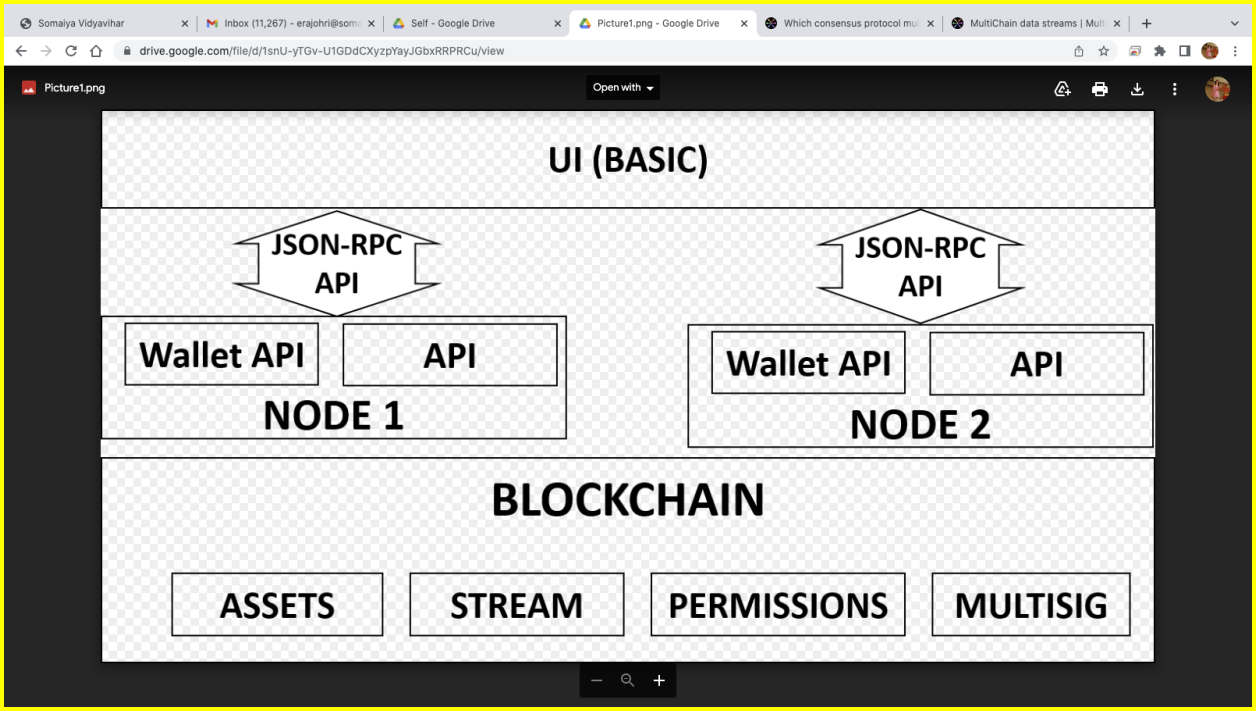
Children

We do not knowingly collect Personal Information from children under the age of 18. In the event you become aware that an individual under the age of 18 has enrolled without parental permission, please advise us immediately.

Changes

We may update this Privacy Policy from time to time and will post such changes on our website, and we encourage you to review it periodically. If any change to this Privacy Policy would change how your Personal Information is treated, then the change will not apply to you without your affirmative consent.

Multichain Architecture:



basic architectural description:

- The two main subsystems of MultiChain are the node (which tracks the chain's global state) and the wallet (which tracks transactions of specific interest to the node and holds private keys). Each of these has separate mechanisms for storing and retrieving information.
- There's no distinction between Bitcoin Core and MultiChain since MultiChain is an extended version of Bitcoin Core.
- You can have multiple instances of MultiChain connected to the same chain.

- The chain contains information permissions, assets and streams, although nodes also read and write these.
- Each node has its own API which can be connected to from an application.
- There is no API to MultiChain in general, only to specific nodes.
- And each node has a separate API which is what each UI can connect to. There is no such thing as connecting to the "nodes" in general.

Consensus Protocols multichain use:

Distributed consensus between identified block validators. It's close in spirit to something like PBFT (Practical Byzantine Fault Tolerance), but instead of multiple validators per block, there is one validator per block, working in a round-robin type of fashion.

What happends if one validator in the round-robin type fashion failes? Does it time-out and re-assign another validator/proposer in the same round-robin type fashion?

E.g.

Round 1
Proposer/Validator: NewHeight -> (Propose -> Prevote -> Precommit)+ -> Commit

Error condition: Proposer/Validator Fails at Precommit.
No Impact for the validator nodes right? As long as the majority of the validators have received the prevote.

Otherwise if a validator/proposer fails in a round-robin type scheme
Re-round is performed and another validator/proposer is picked right?

NewValidator/Proposer: NewHeight -> (Propose -> Prevote -> Precommit)+ -> Commit

** First it should be noted that it's not a propose -> prevote -> precommit type of consensus algorithm, but rather a stochastic consensus algorithm where rollbacks can happen in the event of a conflict – just like bitcoin.

In practice if you use set mining-turnover=0 and validators don't override that, a rollback can only happen in the event of a validator failure.

If a validator fails, i.e. too much time has passed, other validators who were not part of the self-selected rotation will step in after a random time delay. Usually one will outright win and become part of the new round robin set. If not, there's a fork which will be resolved by whichever validator was next in the rotation.

Multichain Data Streams:

Source: https://www.multichain.com/developers/data-streams/