Blockcurr: A Blockchain-Cryptocurrency System

A. Jain
info@blockcurr.com
blockcurr.com

Abstract: Blockcurr is a novel blockchain-cryptocurrency application platform. It consists of decentralized application infrastructure for creating blockchain applications supported by cryptocurrency payment options. Blockcurr facilitates transaction processing with enhanced data security, auditability, and transparency across all its platform tiers thereby improving trust amongst anonymous participants. It incorporates digital identity to authenticate users, performs transaction verification, its provenance, and record asset and value exchange on a distributed ledger. This is instantly shared across peer-to-peer network with self-enforcing smart contracts eliminating the technical dependency common with a single ledger system. Through better design of robust decentralized consensus protocol and instant execution, the distributed ledger technology is able to achieve faster throughputs. This is useful to automate governance rules for autonomous processing of transactions involving multiple party blockchain agreements.

Getting the right blockchain platform to work with is a key a requirement of an enterprise with flexibility to build blockchain applications and launch new business models. We offer open APIs and SDKs that developers would find practical and useful for cross platform application development and interoperability with external systems.

There are a number of companies implementing Blockcurr into their solutions. Based on these experiences, we identify a number of design considerations used by Blockcurr to support business requirements and provide the technology blueprint that you could use to launch your innovative ideas on blockchains.

Introduction

Develop decentralized application, deploy and test, and rollout solutions on blockchain network are three important activities that organizations perform to target opportunities with blockchains. All three are generally the focus with blockchain technology providers to promote the creation of decentralized business models. There are many examples from companies that have launched initial coin offering to encourage the use of their apps leveraging cryptocurrency and blockchain infrastructure. However, while cryptocurrency has been the subject of rigorous regulatory investigation in the blockchain industry, the blockchain community has placed considerably less attention on ways that this technology can support existing regulations and industry standards, to create better economic environment that transcends boundaries and improves the quality of life for all participants.

Designing blockchain technologies to promote disruption is a worthwhile goal for numerous reasons. Current business models are centralized and seem to favor a few individuals, organizations, people in power or those with tremendous wealth. The computing technologies in vogue support centralized deployments on cloud, big data, and mobility infrastructure. These have proven ineffective because of the number of layers and intermediaries involved to process and deliver information in meaningful ways. There are also technological challenges related to mining, development of self-learning capabilities useful for artificial intelligence solutions, autonomous systems, and self-governing exchanges.

Similar to how any prior technology has been used to improve and reward business outcomes, we believe blockchain offers an interesting area of research to explore its suitability for building digital information exchanges and decentralized autonomous organization (DAO). These are models for new economy that would use blockchains and cryptocurrency.

Blockcurr

To better understand how Blockcurr technology can play a critical role in launching decentralized applications and business models, we provide a brief background of Blockcurr platform and its core components used to support blockchain and cryptocurrency ecosystem.

First, Blockcurr provides blockchain computing technology with functionality to build software applications. This includes blockchain platform to create blockchain transactions and digitize assets, services to build and deploy smart contracts, digital wallets for storing data and cryptocurrency, capability to securely transmit, receive, and process transactions over a decentralized peer to peer network. Next, Blockcurr provides dockers to secure and forward information to specific locations, flexibility to connect workflows and configure blockchains to suit specific domains, and open APIs to build blockchain based cloud and mobility solutions. It provides transaction security and proof of ownership for trading. You can also share and store blockchain data on the network or local hardware.

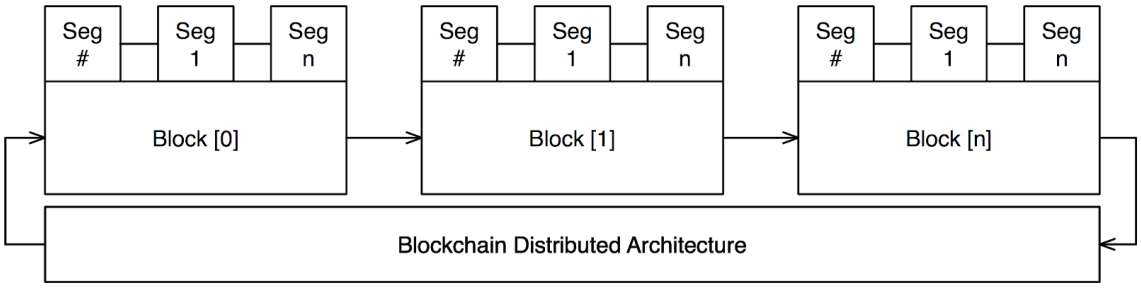
The primary components of Blockcurr system are:

- 》 Blockchain Platform
- 》 Docker
- 》 Accounts
- 》 Distributed Ledger Technology
- 》 Cryptocurrency and Tokens
- 》 Transactions
- 》 Databases
- 》 Kernel
- 》 Peer-to-Peer Network
- 》 Decentralized Distributed System

Each of the components provide an explanation of the protocol, architecture, code, features, and samples to build and run blockchain applications. These are covered in the following sections.

Blockchain Platform

Blockchain platform architecture consists of a data structure with one or more connected block segments with identifiers, and programs linked together on a blockchain distributed architecture. Blockcurr codecs further secure digital assets, contracts and transactions as they get prepared for transport and sharing with other peer nodes.



The elements of a generic blockchain are as follows:

- Segments: These provide unique identifiers to denote user accounts, senders and receivers, transaction sets, timestamp, nounce, external tokens, and state to package inside a blockchain.
- Blocks: These contain identifiers for wallets, ledger and chain links.
- Blockchain: This layer provides the block address and cryptography codecs to build segments, blockchains, and digital signatures.

Blockcurr's special purpose blockchains provide additional capabilities for data storage, creation of cryptocurrency and tokens, business logic and workflow integrations, programs and smart contract execution, and for interoperability with cryptocurrency exchanges.

The blockchain application platform is easy to use and provides seamless integrations with underlying infrastructure to build and deploy applications on Blockcurr network.

Docker

Blockcurr's docker is used to store digital assets and cryptocurrency. It is made up of several key elements such as blockchain, domain signature, wallet, passcode, and security codecs.

Docker provides:

》 Container for storing digital assets
》 Proof of creation and provenance
》 Support for blockchain transaction and smart contract protocols
》 Strong user privacy, identity verification and authentication protocol
》 Strong security for transactions, payments, and data
》 Fast validations necessary to send and receive data and payments
》 Tamper proof digital signature scheme
》 Mechanism for certifying autonomous data sharing

Docker allows developers to digitize, store, and share data with multiple parties linked to smart contracts and makes it available when required for processing with blockchain transactions.

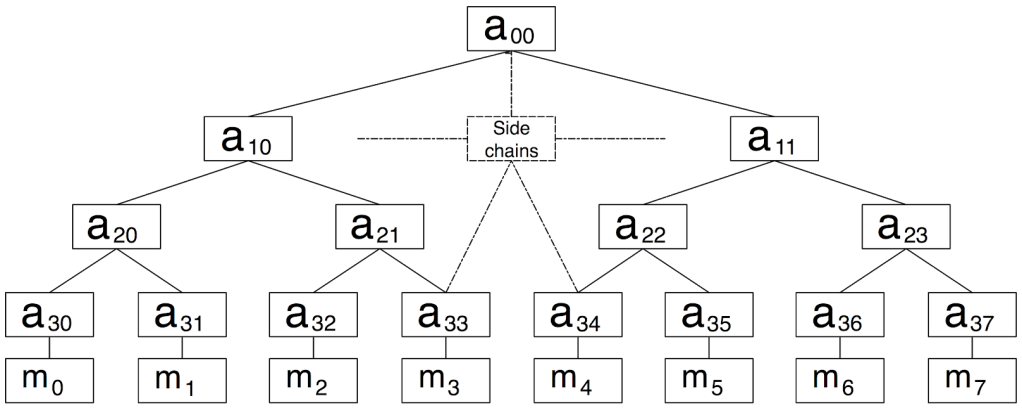
Accounts

In Blockcurr, a blockchain is created to manage account profiles for users, entities and devices. It includes identity validations for user documents supported by verification levels and utilizes tokens for devices. Each account is assigned a wallet with blockchain identifiers, and crypto codes essential to maintaining privacy of accounts at all times. Account information is used to verify trades, token ownership, transaction ledgers, data access and controls.

Once an account is created, it provides users access to blockchain transactions and their data.

Distributed Ledger Technology

Blockcurr consists of a distributed ledger technology with decentralized identity management solution for sharing data among peers in the network. The ledger provides a time-ordered sequence of transactions, is immutable and publicly verifiable. The hash chunks are cryptographically-secure to ensure integrity of blockchain, prevent tampering and misuse. Each peer also maintains a copy of the ledger. All transactions are validated by peer nodes against Blockcurr's blockchain protocol; updates to the blockchain and final states are made autonomously with consensus among participating nodes on the network.



Temporal slice of Merkel forest

Illustration shows standard model of Merkle binary tree with vertices (a_{ij}), intermediate nodes and leafs computed. The root node summarizes its child hashes, same is the case with intermediary nodes, and leaf summarizes data block hashes.

$$a_{ij} = n(a_{i+1;\,2j}\ a_{i+1;2j+1}), \quad i \in \{0, ..., k-1\}, \quad j \in \{0, ..., 2i-1\}, \quad a_{k,j}\ for\ j \in \{0, ..., 2^k\text{-}1\}$$

Blockcurr ledger implementation is based on extended Merkel Tree with novel construction of poly hash signature scheme that is collision resistant and supports temporal authentication. This provides faster validation, verification and auditability of transactions and digital documents on the network. All block segments of a Merkle tree have a unique hash with corresponding hash identifiers. As more blockchains are created, the hash data is linked to the transaction blocks as branches progress sequentially, in blocks, and as more

leaves get added dynamically. The trees can grow sequential to quintillion blocks and increase by the same amount thus offering a large spectrum to record transactions. Trees can also grow sideways depending upon the implementation with smart contracts and DApps.

Blockcurr's distributed ledger technology allows the creation of blockchain registry to manage personal information, store digital content and their value - securely and anonymously. It serves as a valuable resource for managing the digital rights of users and their digital assets. The ledger features reconciliation, audit reports, and data access controls providing users complete control of their personal information. By simplifying the process of verifying and tracking ownership it makes the authorized data instantly transparent to all parties thereby lowering the cost to transfer assets.

Cryptocurrency and Tokens

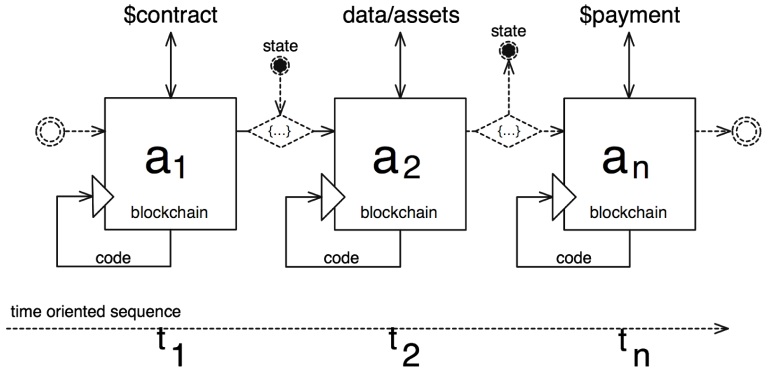
Blockcurr allows creation of custom cryptocurrency coins on its platform. All coins comply with Blockcurr's blockchain specification. These coins can be used for a variety of purposes such as currency, contracts, loyalty reward points, and in-game assets. They can also be redeemed for a service an issuer will provide at a later date. You can peg your coin or token value to another currency such as Bitcoin and Ethereum. Coins and tokens issued can also be easily verified to ensure ownership and redemption transactions.

The foundation for the new economic models with blockchains are based on incentivization using utility and security tokens. These can be traded on exchanges and open up wealth of opportunities to all participants including accredited and non-accredited investors.

Initial coin offering platforms provide a listing of companies and their tokens, encourages blockchain technology advancements and make it easy for entrepreneurs to raise capital from people around the world for their novel ideas.

Transactions

Blockchains have evolved from being distributed database to full fledged transaction chains that involve data, contracts, and business process interactions with various entities. The processing of these transaction chains at peer nodes could be coordinated with other local and network resources and support permissionless and permissioned blockchains. While these do not involve intermediaries, in the case of permissioned blockchains, multiple parties could be involved depending upon the conditions stipulated in transaction contracts.



Blockcurr: Blockchain Transaction

Blockcurr transaction involves the use of several integrated technology, some of the main ones are as follows:

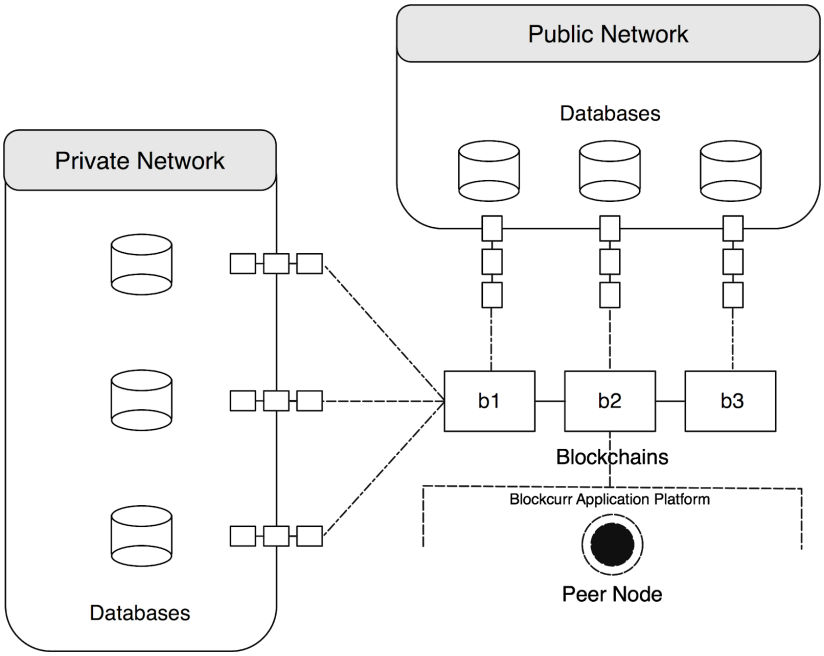
- Blockchain Platform: This issues blockchains for transactions.
- Cryptography: This consists of industry grade cryptography standards to secure data and transaction chains.
- Digital Signature: This is used to certify blockchain origins.
- Wallet: This is used to store digital currency, transactions, and digital assets.
- Passcode: This is used to secure user accounts and digital assets.
- Distributed Ledger Technology: This is used to record all trades, blockchain transactions, and manage account balances.
- Peer Node: This provides capabilities for real-time processing of blockchains and communications with other nodes. Each node supports distributed transaction processing capabilities and more nodes can easily be added to scale throughputs with growth.

Establishing decentralized application interactions with private blockchains and peer nodes is another important feature of the platform so that transaction chains can be seamlessly integrated with enterprise systems.

Blockchain Databases

Blockcurr supports the use of shared public and private databases to record blockchain transactions deployed on a decentralized peer to peer network. Some of the databases that it interfaces with are follows:

- Transaction db: Records transactions amongst participating nodes.
- Trading db: Records trades on exchanges.
- Storage db: Stores of digital assets.
- Machine Learning db: Stores data from learning and predictive systems.
- Cognitive db: Provides fast intelligence and smart assistance to participating nodes and external networks.

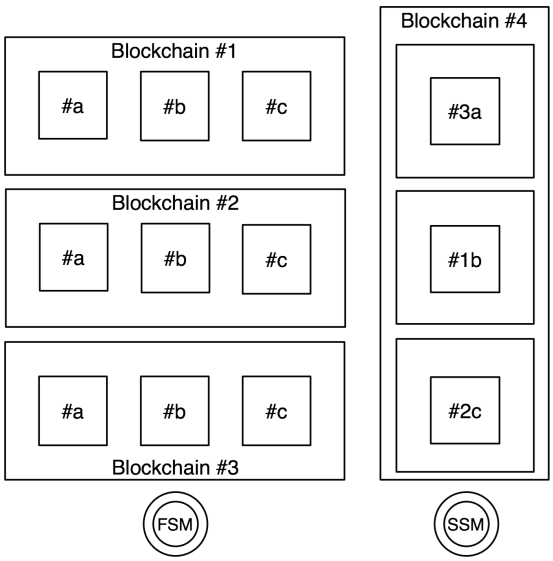


Blockcurr provides open API's to connect with databases, big data solutions, and mobile applications so that you can leverage the full capabilities of blockchain application platform leveraging content and data from your internal IT systems.

Kernel

Blockcurr Kernel contains programs that operate as a network of virtual computing resources that are globally accessible to run state machines and programs to execute smart contracts and transaction processing. Data from one or more block chains can be combined to create new blockchains or to model behavior of system based on the state. Blockcurr connects with one or more participating nodes and network protocols for consensus and data sharing, provides access point for services and decentralized applications with built-in economic functions.

Cryptography core utilizes bit-level, randomized bit-wise, and session based key algorithms for computing blockchain hashes and encryption functions for variable block lengths, ciphers, and symbols with no restrictions. Additionally, many other algorithms are made available to enhance the security even further with the goal to deliver an optimal balance between security and time to encrypt and decrypt blockchain streams.

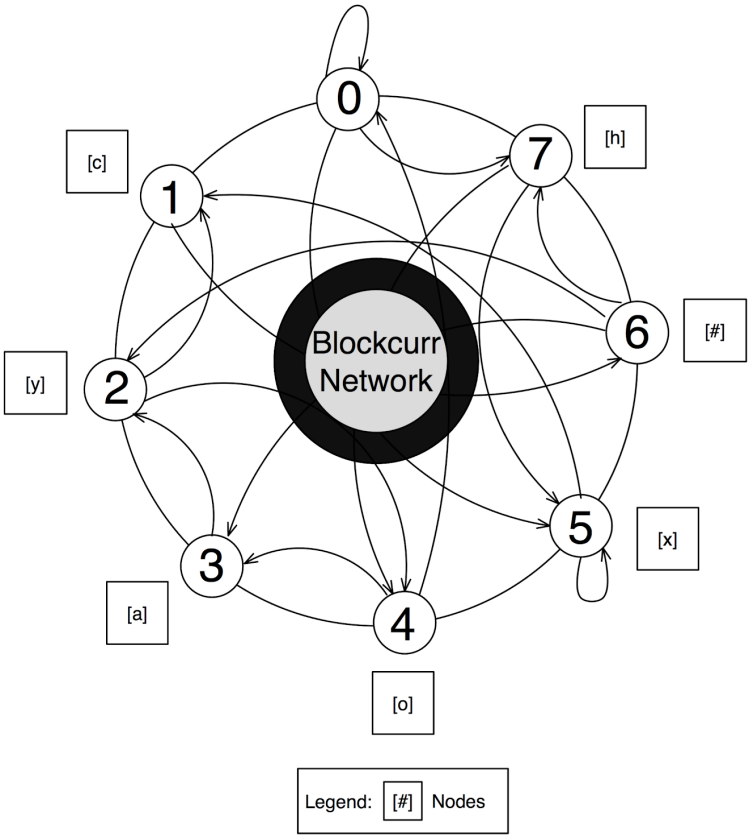


Finite State Machine (FSM), Smart State Machine (SSM)

Blockcurr's compact code results in fast software implementations of peer nodes with discrete blockchain processing capabilities and distributed computing power to match the transaction processing needs. It is particularly suitable for cryptographic applications where transaction volume is large and faster response times are essential for trade confirmation in a distributed network.

Peer-to-Peer Network

Blockcurr peer-to-peer network consists of nodes integrated into a mesh architecture as illustrated below. A node can run multiple instances, each contains programs to run blockchain algorithms, operate peer exchanges and execute transactions. The network topology facilitates seamless coordination with other nodes to communicate, send and receive messages, search and query databases, and interact with cloud and mobile applications.



Node: A node on a peer-to-peer network is linked with other nodes within the same environment, or deployed within a mesh architecture to perform various functions such as validate transactions, verify payments, facilitate consensus, and secure communication channels.

Decentralized Distributed System

Blockcurr decentralized distributed system consists of computing resources operating on a distributed hardware and software architecture. All nodes can easily be replicated and extended, have built-in fault tolerance with features to execute smart contracts and multi-party interactions, send and receive messages to each other over HTTP(S) and TCP/IP transport protocols.

The characteristics of decentralized network are as follows:

- Consistency: All nodes in a distributed system are automatically synchronized, and have the latest copy of transaction data.
- Integrity: Maintain reliable record of transactions, communications, and messages in a tamper-proof way, protecting the system and ensuring survival from security threats.
- Consensus: Each node operates independently to validate and verify data following consensus protocols across multiple endpoints.
- Fault Tolerance: Built-in redundancy and robustness ensures the distributed system continues to operate and transition workloads without halting while allowing the failed endpoints to recover automatically.
- Availability: The system is available and accessible with 100% uptime.
- Accountability: Maintain accountability and improve performance through audit trails and active profiling of network data streams.
- Transparency: Maintain complete transparency between trusted network endpoints by sharing latest information on ledger, transactions, and state information.
- Security: Provides multiple levels of security and monitoring at each node with cyber defense techniques that restrict access to sensitive information and ensure privacy of communication channels over public and private network protocols.
- Self-organization: The system can be configured for single and multi-node processing of blockchain data streams, additional rules can be defined to service transaction chains, and monitors can be configured locally to manage the nodes independently or coordinate with other peer nodes on the network.

Summary

The work presented in this white paper sought to uncover how Blockcurr could be used to support development of decentralized applications, new business models, and to innovate enterprises. The platform provides a system for building DAO networks and does not require massive investments in computational resources. The solution is robust, simple to implement and supports interoperability with other public blockchain platforms.

Blockcurr's kernel provides the core infrastructure necessary to create blockchains, tracking assets, digital signatures, securing event streams, and cryptocurrency, providing complete control of the environment and accelerating the pace of application development. The account over spending problem is eliminated through automated proof-of-amount verification of transactions and consensus protocols at the nodes as they occur. The innovations in ledger design and codecs make it computationally complex for nodes to make any changes on their own. There are additional provisions for self regulation of peer nodes that permit blockchain and smart contract processing without requiring any intermediary or network coordination. Blockcurr nodes can be easily added or removed to scale with the growth of blockchains across public or private networks.

Future work: Blockcurr technology presented in this paper provides all the building blocks to help you make the most of blockchain computing technologies. To implement blockchains, we discussed some of the key components and architecture that are essential to develop ideas for your enterprise and leverage our experience and findings to innovate business models. Our work continues to focus on building and providing you the core technologies that can make a meaningful impact in this fast emerging blockchain ecosystem that can potentially benefit everyone.

Additional sources

List of papers that discuss many of the concepts important to the future with blockchain.

1992 Tim May. The Crypto Anarchist Manifesto

1997 Adam Back. Hashcash

1997 Nick Szabo. Formalizing and Securing Relationships on Public Networks

1998 Dai, Wei. “B-Money”

2002 Adam Back. “Hashcash - A Denial of Service Counter-Measure”

2003 Jain, A. & Juneja, N., Business Services Network, The 2nd generation Web

2005 Hal Finney, “Reusable proofs of work”

2008 Satoshi Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System

2013 Vitalik Buterin. Ethereum. Bootstrapping A Decentralized Autonomous Corporation

2015 Bohme, Rainer, Nicolas Christin, Benjamin Edelman, and Tyler Moore. Bitcoin: Economics, Technology, and Governance, The Journal of Economic Perspectives 29, 213{238.

2016 Raskin, Max, and David Yermack. Digital currencies, decentralized ledgers, and the future of central banking, National Bureau of Economic Research.

2017 Aune, Rune Tevasvold, Maureen O'Hara, and Ouziel Slama, Footprints on the blockchain: Trading and information leakage in distributed ledgers, The Journal of Trading.