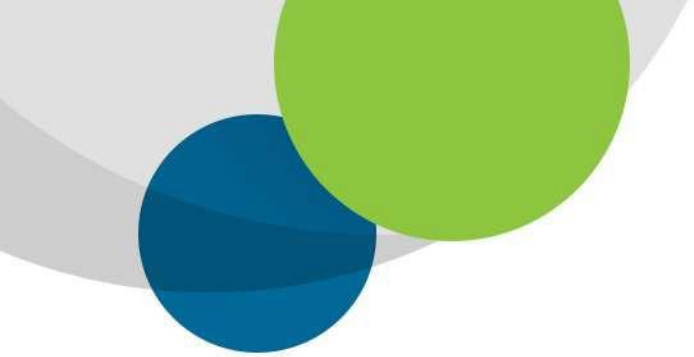

The Blockchain Landscape

Dr. Arati Baliga

Office of the CTO

Contents

Executive Summary

The Bitcoin invention by Satoshi Nakamoto in 2008, and its subsequent gain in popularity a few years later has highlighted the core computer science invention powering Bitcoin, which is the blockchain. The blockchain technology allows for maintenance of a shared distributed ledger (also known as the blockchain), which can be simultaneously read and modified by all involved parties but is not owned by any party. This can be implemented with absolutely no trust, as in the case of Bitcoin, or limited amount of trust, as in the case of consortium blockchains, where a group based consensus mechanism is used to update the shared ledger. Since then, the sheer power of the blockchain technology has inspired and fueled an entire ecosystem around it, focused on fully unleashing its potential. This area has had exponential growth in the past couple of years, leading to a number of platforms, applications, startups, projects and research around this new invention. This document focuses on scoping the existing platforms specifically for developing new blockchain-based applications. It also discusses some use cases that can be built using the platforms in the areas of e-governance, healthcare and payments.

Bitcoin Overview

The Bitcoin protocol allows users to exchange of the *Bitcoin* (BTC) cryptocurrency without any trusted third party using the decentralized, peer-to-peer Bitcoin network. The record of the transfer is maintained in a public blockchain, also known as the Bitcoin blockchain. The blockchain is replicated on every node that participates in the Bitcoin network. Each user in the Bitcoin network installs a Bitcoin client, along with a Bitcoin wallet that stores the public/private keys generated for that user. The Bitcoin wallet stores the private keys locally on the users' computing device and encrypts it with a password. Whenever the user wants to pay others using Bitcoins, the wallet software allows the user to make a payment by specifying the payee's Bitcoin address. The Bitcoin address for each Bitcoin user is derived by double hashing his public key.

Bitcoin Network: When a node comes up, it has a list of nodes that are pre-set that it contacts. Starting from these nodes, it actively discovers new nodes by exchanging neighbor lists with each node that it knows. This exchange helps each node grow its neighbor list and continues until an unstructured peer-to-peer network is formed where each node talks to a large number of others nodes in the Bitcoin network. The nodes on the overlay network are contacted for broadcasting transactions and other messages in accordance with the Bitcoin protocol.

Bitcoin Transactions: A Bitcoin transaction is initiated when User A on the Bitcoin network wants to pay User B, X amount of BTC. The client software forms a transaction that is signed by User A and includes User B's Bitcoin address representing his intent to transfer X BTC to User B. This transaction is confirmed, when it gets included in the Bitcoin blockchain, which generally takes around 10 minutes. For a transaction to be considered completely secure, it has to have six confirmations, which takes about an hour. A block represents a fixed number of transactions that are included within it. It also includes a special kind of transaction known as a coinbase transaction that represents a payment to the miner of the block of Y BTC, where Y represents the mining reward for mining a block at that point in time. Currently, the mining reward is 25 BTC.

Mining and Proof-of-Work: The blockchain is appended with blocks that include transactions. The Bitcoin blockchain is permissionless, which means any node within the Bitcoin blockchain is able to add blocks into the blockchain. To add blocks to the blockchain, the node has to show that it has performed some amount of work, also known as Proof-of-Work (PoW). In Bitcoin, the node has to find a hash value that is less than a certain number, also referred to as the difficulty level that is dynamically tuned by the Bitcoin protocol. The process of solving this PoW puzzle to find a winning hash value is known as mining. The node that is the first to find the winning hash is the one that gets to add the block to the blockchain and also claims the mining reward. Due to the distributed nature of this process, it sometimes happens that more than one node is able to find the winning hash at the same time. In such cases, each winning node will add a different block to the blockchain, temporarily generating a fork in the blockchain. However, as more blocks are added to these forks, the protocol will ensure that the branch with the maximum PoW will be the one that will get included in the blockchain and others will be discarded, leading to an eventual consistency among all nodes regarding the state of the blockchain.

Bitcoin Blockchain Features

The Bitcoin Blockchain is the shared ledger, which can be read and modified by all involved participants in the blockchain. It has the following characteristics.

- **Public ledger** - Any node with a Bitcoin client can read or add transactions to the ledger.
- **Permissionless entry** - The miner who has solved the Proof-of-Work is the node that will finalize a block representing a set of transactions in the ledger. Any node can be a miner by solving the PoW puzzle successfully.
- **Proof-of-Work** – Bitcoin uses the computation of the hash with a certain difficulty level as a Proof-of-Work measure.
- **Customizable fields** – The structure of the blockchain is fixed. Each block has a number of transactions with some meta-data where the user can add some information.
- **Native token** - The native token of the Bitcoin blockchain is the Bitcoin, which is also the cryptocurrency that is moved between users. Bitcoins and transaction fees in Bitcoins are awarded to the miner mining a particular block.

The Blockchain

While Bitcoin used the blockchain to implement a cryptocurrency system, it can be generically applied in other scenarios, with or without using a native token. The blockchain offers several features that make it an enabler for new applications that were either tedious or impossible to implement in its absence.

Blockchain features

Below we highlight some of the key properties of the blockchain.

- **Cryptographic guarantees** – All transactions on the blockchain are signed by end-users. This cryptographic guarantee allows for verification of the transaction with the user's public key. Signing guarantees the authenticity, integrity and non-repudiation of that transaction.
- **Pseudonymity** – Each entity within the blockchain network transacts with a generated address, which does not reveal the real identity of the user. This allows a certain amount of privacy on all transactions.
- **Immutability -** The transaction broadcasted to the blockchain network has to be confirmed and included as part of the distributed ledger. Once confirmed, the transaction cannot be changed and stays in the ledger forever. No entity can delete or rollback transactions once they are included as part of the distributed ledger.
- **Shared Read and Write –** The blockchain is either public or private within a limited set of entities. All concerned participants have visibility into the blockchain and can independently verify any transaction within it. All participants can generate transactions that can be added to the shared ledger.
- **Auditability and Transparency –** All transactions on the blockchain are validated and timestamped after the transaction is verified and included in the distributed ledger with distributed consensus. This accounts for a global truth that any node in the future can verify and no node in the network can change

the data that is part of this distributed ledger. This improves accountability as well as transparency for the data that is included in the blockchain.

- **Distributed ownership -** In case of public blockchains, no entity owns the blockchain but all of them can add to the ledger and validate transactions. In a consortium blockchain, all participants own the blockchain equally and they can change the ledger by a super-majority of votes or other forms of distributed consensus algorithms.

Permissioned versus permissionless blockchains

Blockchains can be built similar to a Bitcoin like system where anyone can read the blockchain data, add entries to it and any node can extend the blockchain by finalizing blocks. Such a blockchain is known as a permissionless blockchain. On the contrary, in a permissioned blockchain transaction processing and extension of the blockchain can be performed by a set of known and accepted nodes. Permissioned blockchains are attractive in cases, where transaction-processing nodes need to be known to comply with regulations, as in the case of financial institutions.

Permissionless blockchain data is public. However, it is not necessary that permissioned blockchain data needs to be private. Permissioned blockchains can be made public, e.g., if financial institution data needs to be made available to regulators to check for compliance. Making blockchain data available to consumers or clients provides the real benefit that blockchain technology provides, which is transparency and auditability.

With permissioned blockchains, generally a native token is absent, so is the process of mining and the mining reward. Since the transaction processors are known entities, other real-world incentives are used to facilitate transaction processing. Each transaction processor gets its turn to add a block in the blockchain. To increase the security of the permissioned chain, hashes of block headers are intermittently submitted to a permissionless chain, publicly available, such as Bitcoin. This increases the security of the permissioned blockchain against attacks where multiple entities are colluding together to create forks in the permissioned blockchain.

Blockchains versus databases

Blockchains are blocks of transactions chained together. Transactions work on some data, for example, account balances. Traditionally, such operations are carried out using databases, where data is stored within the database and transactions read or modify the data held within the database. Blockchains allow for similar operations but really are very useful when the system requires multiple writers to the same database and there is no notion of trust on the operators. Blockchains also provide immutability and transparency on transactions that have already happened, along with cryptographic guarantees on every single transaction. Blockchain systems are also automatically decentralized and therefore resilient to failures, security compromises and failures of individual systems.

Key Concepts

This section introduces some of the key concepts with blockchain technology that are commonly used in newer blockchain platforms (also referred to as Blockchain 2.0). This is to aid the reader in understanding the merits of these newer systems.

- **Simple Payment Verification (SPV)** - Simple payment verification allows lightweight clients to check if a given transaction is included in the blockchain. A lightweight client is an implementation of the blockchain client on a low powered device, such as the smart phone. The lightweight client does not download the entire blockchain but only downloads the headers of the blocks to perform this verification. Though initially introduced with Bitcoin, this concept can be generalized to other blockchain platforms as well.
- **Pegged Sidechains** – Sidechain is a separate blockchain that interoperates with the main Bitcoin blockchain. A separate sidechain allows for faster innovation of new applications without polluting the main Bitcoin blockchain. It however allows for users to quickly transfer Bitcoins to the sidechain and the other way round by forming a two-way peg to interoperate with the main Bitcoin blockchain. The transferred Bitcoins from the Bitcoin network can be converted into the cryptocurrency used by the sidechain. While they are in circulation on the sidechain, those Bitcoins are immobilized in the Bitcoin blockchain.
- **Blockchain Anchoring** – This technique is used generally by permissioned blockchains to periodically submit hashes of their block headers into a permissionless chain, like Bitcoin. This inclusion allows users of the permissioned chain to verify the hashes that are validated and included by miners in the permissionless chain. Anchoring strengthens the immutability guarantees of the permissioned blockchain.
- **Merged Mining** – Merged mining is a technique that enables to use the same mining equipment on multiple blockchains. For example, a miner using the Proof-of-Work hashing technique can use it to mine Bitcoins on the Bitcoin network as well as Namecoins on the Namecoin blockchain. This is possible because the Proof-of-Work technique used in both blockchains is the same.
- **Proof-of-Stake (PoS)** - This is an alternative to Proof-of-Work. Proof-of-Work requires the miner to compute a large number of hashes until he has produced a winning hash or mining for that particular block has ended. Proof-of-Stake gets rid of the wasteful hash computation and instead uses the stakes owned by each node in the network as a share to mine blocks proportionately. For e.g., with a blockchain system using the PoS protocol, if a miner holds 1% of the total Bitcoins, he is allowed to mine 1% of the blocks.
- **Proof-of-Burn** – This is an alternative to Proof-of-Work and Proof-of-Stake. Proof-of-Burn is used to show that the miner has done something really hard without expending real resources like electricity. Proof-of-Burn involves burning the currency by sending it to an unspendable address. It can also be used as a technique to transition one cryptocurrency into another one. For example, when X amount of Bitcoins are burned in the Bitcoin network, an alternative interoperable network can verify that the transaction has confirmed and instantiate Y amount of its native currency to that user, equivalent to X Bitcoins.

Blockchain Platforms

Unprecedented growth and interest in blockchains has led several companies and public foundations to develop blockchain platforms that are mostly open sourced and available for all to participate and use. These platforms allow for rapid prototyping, development and deployment of new blockchain applications. Each blockchain platform is designed with specific goals, which dictate its features. We broadly categorize the platforms available in five different categories:

- **Bitcoin based meta-data platforms –** Designed to leverage the already adopted Bitcoin blockchain. These platforms allow for allotment and transfer of custom assets using the Bitcoin blockchain.
- **Blockchain platforms for financial applications –** Also known as FinTech blockchain platforms, this category specifically targets applications within the financial domain.
- **Smart contract platforms -** These platforms mainly focus on applications that require complex logic beyond just expressing account balances and balance transfers as in the case of cryptocurrency transfers.
- **Consortium/Enterprise platforms –** Target enterprises and consortiums that wish to take advantages of the blockchain, but in a more controlled manner. These also typically use a distributed consensus protocol, getting completely rid of PoW and mining.
- **Sidechain platforms -** Sidechain platforms allow for faster innovation without polluting the main Bitcoin blockchain or incurring its overhead. Sidechains allow for building alternate chains that operate via a two-way peg into the Bitcoin blockchain or as an anchored chain.

Bitcoin based meta-data platforms

The goal of Bitcoin based blockchain platforms is to use the already widely adopted Bitcoin blockchain itself to realize new kinds of applications. These platforms add meta-data into transactions on the Bitcoin blocks, where the meta-data has a specific meaning. For e.g. a company can issue tokens to its employees where the tokens can be translated into points to be used for redemption. Since these systems shown in Table 1 below encode data within the Bitcoin blockchain, they use the same ledger used by Bitcoin and inherit the same properties from the Bitcoin system, such as Proof-of-Work, mining, etc. The transactions are processed by the same nodes, which process the Bitcoin payments. All platforms use the OP_RETURN instruction to encode the meta-data in the transaction.

Table 1 shows some notable platforms using the main Bitcoin blockchain that allow for developing new blockchain applications, which allow registering and transfer of custom assets, such as smart property, coupons, movie tickets, or financial assets such as stocks, bonds, etc. These assets are basically IOUs from the issuer that the end users trust. The system itself cannot do anything if the issuer does not hold up to his promise of delivering the real world asset.

Platform	Blockchain Domain	Source Code	Native Token	Currency Agnostic	Wallet Support	API Support
ColoredCoins	Smart property, coupons, assets, etc.	Open	BTC	✗	✓	✓
Coinprism	Stocks, currencies, smart property	Open	BTC	✗	✓	✓
CoinSpark	Asset transfer	Partially Open	BTC	✗	✓	✓
ChromaWay	Custom asset transfer	Partially Open	BTC	✗	✓	✓
Omni	Asset transfer, property, financial	Open	Mastercoin	✗	✓	✓

Table 1: Bitcoin based meta-data platforms

ColoredCoins [1] – ColoredCoins platforms uses the Colored Coins protocol, lets the user create digital assets on top of the Bitcoin blockchain by using the Bitcoin 2.0 protocol. Both the platform and the protocol were developed by Colu. These assets are encoded in the metadata of Bitcoin transactions and represent real world value. The asset can be anything of value, commodities, financial assets, store coupons, tickets, etc. Colu also offers other products that are not open sourced that are based on the colored coins protocol.

CoinPrism [2]– CoinPrism developed an Open Assets Protocol for implementing, issuing and transferring any kind of custom asset on the Bitcoin blockchain. The Open Assets Protocol is completely open sourced and available for use for anybody wanting to integrate with existing systems. Coinprism's web wallet implementation use the Open Assets protocol to allow users to issue and transfer custom assets.

CoinSpark [3] – CoinSpark from Coin Sciences enables similar functionality of adding meta-data to Bitcoin transactions. Some of the built-in functionality involves asset creation and transfer, notarizing important emails and attaching messages to transactions. It also has support for development, with libraries available, in seven programming languages and wallet API. It uses a different approach for encoding assets but has lot of similarities with Coinprism's OpenAsset protocol.

ChromaWay [4]– ChromaWay has an enterprise platform for colored coins and ChromaWallet, which is a ColoredCoins wallet . It uses a different protocol known as Enhanced Padded Order based Coloring (7) [26] to embed the asset within the Bitcoin blockchain.

Omni [5]– Previously known as Mastercoin, Omni provides a fully decentralized trading of assets and digital property using the Bitcoin blockchain. Notable applications that use the Omni layer are the Factom chain, which is a blockchain for recordkeeping and LaZooz, a ride sharing service on the blockchain.

FinTech platforms

Blockchains have direct appeal to financial markets. This segment has grown the most where investment in the FinTech sector has probably been the largest compared to any other areas. Lots of platforms focus on finance applications, such as clearance and settlement, derivatives, equity, foreign exchange, payments, etc.

Table 2 lists the platforms available specialized for the financial domain.

Platform	Ledger Visibility	Ledger Type	Source Code	Uses Bitcoin Blockchain?	Consensus Method	Native Token	Currency Agnostic	Mining	API Support
Ripple	Public	Permissioned	Partially Open	✗	Ripple Consensus	XRP	✓	✗	✓
HyperLedger	Private	Permissioned	Not yet open	✗	HyperLedger Consensus	None	✓	✗	Not yet
Counterparty	Public	Permissionless	Open	✓	Proof-of-Work	XCP	✗	✓	✓
Stellar	Public	Permissionless	Open	✗	Stellar Consensus Protocol	Lumen	✗	✗	✓
Bitshares	Public	Permissioned	Open	✗	Delegated PoS	BTS	✗	✗	✓
Nxt	Public	Permissionless	Open	✗	Proof-of-Stake	NXT	✗	✗	✓

Table 2: FinTech platforms

Ripple [6] – Ripple provides a decentralized distributed network and a protocol that provides plug and play infrastructure for financial institutions. Developed by Ripple (previously Ripple Labs), it specializes in instant transaction verification and settlement, providing a decentralized alternative for RTGS. Users can also settle transactions and perform cross currency conversions automatically where liquidity is provided by Ripple market makers. Users can then get paid in their local currency. The Ripple network records all transactions in a public ledger, known as the Ripple Consensus Ledger (RCL). The ledger is extended by a consensus protocol where a super majority of nodes would have to agree on the transactions that are to be added to the ledger.

HyperLedger [7] – HyperLedger, now acquired by Digital Asset Holdings, provides decentralized settlement via distributed ledgers. The goal of HyperLedger is simply to provide shared replicated ledgers across a group of institutions. It allows for building permissioned ledgers for institutions, where balances and transfers can be kept private. It is built with no internal cryptocurrency, thereby provides lower regulatory risk and no volatility. It also allows for some amount of control on who can create accounts and what jurisdictions they belong to. HyperLedger code is being written and will be open sourced in the future.

Counterparty [8] – Counterparty builds a powerful platform for consumers to perform financial transactions without a trusted third party. It uses Bitcoin as the underlying blockchain platform and works by adding meta-data to Bitcoin transactions. Mining and consensus all follow the same rules as the Bitcoin network. The counterparty platform needs its own currency to run Counterparty applications, such as escrow and clearinghouse. The Counterparty currency, XCP, was created by burning bitcoins. It also supports a Turing complete scripting language to write more complex code.

Stellar [9] – Stellar is an open source payment network for sending any currency or asset without incurring additional middlemen fees. Currency is automatically converted as in the case of Ripple. Stellar is perhaps the closest competitor for Ripple. It uses a unique Stellar consensus protocol, which allows all nodes to reach an agreement regarding the state of the ledger. It adds a lot of flexibility in how nodes can arrive at consensus and sets of nodes to include in the quorum. Stellar currency is also explicitly inflationary, where 1% of new coins are added every year.

BitShares [10] – BitShares is a financial smart contract platform that provides industrial grade speeds. It uses a delegated proof-of-stake consensus algorithm. It provides decentralized asset exchange, user-issued assets, integrated peer-to-peer lending and collateralized bond market as some of the unique features of this platform.

Nxt[11] – Is a decentralized platform for all kinds of financial applications, ranging from digital money, shares, equities, etc. It also allows for other applications such as decentralized voting, asset exchange, and private messaging. Nxt platforms uses Proof-of-Stake for advancing the blockchain, and therefore does not require mining. Block authors are selected in a random order and chosen to advance the ledger. The higher the stake held in the system, higher the likelihood of getting selected for adding a block to the ledger. Since this platform has low computation requirements, it can be run on low-end devices, such as the smart phone and Raspberry Pi platform.

Smart Contract Platforms

Smart contract platforms allow building and enforcing smart contract using the blockchain. Smart contracts are little software programs have the ability to enforce the contract in such a way that the contract itself and its effects on the inputs are completely verifiable. These platforms provide a Turing complete language to express complex logic beyond simple cryptocurrency transfers. Smart contracts have lots of applications in finance as well as in other domains. Smart contracts can enable decentralized applications, such as voting, auctions, lottery, escrow systems, crowd funding and micropayments to name a few.

Platform	Ledger Visibility	Ledger Type	Source Code	Consensus Method	Native Token	Currency Agnostic	Mining	API Support
Ethereum	Public	Permissionless	Open	Proof-of-Work (Hashing)	Ether	✗	✓	✗
Rootstock	Public	--------	--------	--------	Rootcoin	✗	✓	--------
Codius	Public	Permissionless	Open	Codius Consensus	✗	✓	✗	✗

Table 3: Smart Contract platforms

Ethereum [12] – Ethereum is one of the most popular platforms to build and deploy smart contracts, which are stored on the blockchain. Ethereum has support for a Turing complete programming language to write complex code. Each smart contract is stored on the blockchain and any Ethereum node can independently verify its inputs and execution. Currently, it can only support full nodes and each individual node is engaged in mining, which in turn runs the contract code locally.

Rootstock [13] – Rootstock is a decentralized peer-to-peer platform for running smart contracts on top of the Bitcoin blockchain. It implements the smart contract platform as a sidechain and adds value to the main Bitcoin blockchain by allowing users to write more complex smart contracts. This platform is currently work in progress and should soon see an official launch.

Codius [14] – Codius from Ripple, is an open source, hosting platform for decentralized services, decentralized apps and smart contracts. Smart contracts reside and execute on sandboxed environments within smart oracles. Codius uses Javascript as the scripting language eliminating the need to learn custom programming languages. It has an in-built payment system where users as well as applications can pay each other. Though the code is open sourced and available, Ripple is no longer contributing to this platform because of lack of demand.

Consortium/Enterprise Platforms

Consortium platforms are built for a group of entities to maintain a blockchain, read update and share the data in a trustworthy manner. In such platforms, there is some notion of trust. The penalty for breaking the trust is enforced by other means, such as legal contracts with the enterprises. Such platforms get rid of the wasteful Proof-of-Work computations and consensus is achieved by a super majority of the peers within the group, where each enterprise or entity maintains a mining node that will participate in the consensus process. These platforms also allow enterprises to define their own rules and block structure.

An example use case for this type of platform would be a federation of companies maintaining a blockchain to share order information for product cross-promotion.

Platform	Ledger Visibility	Ledger Type	Source Code	Consensus Method	Mining	Currency Agnostic
MultiChain	Public/ Private	Permissioned/ Permissionless	Open	MultiChain consensus	✗	✓
OpenChain	Private	Permissioned	Open	OpenChain consensus	✗	✓
BlockStack	Private	Permissioned	Closed	Approval by super majority	✗	✓
Chain	Private	Permissioned	----	----	----	----

Table 4: Enterprise/Consortium Platforms

MultiChain [15] – MultiChain is the first platform to build a permissioned blockchain. It allows the shared ledger to be as open or as closed as required. Mainly directed towards enterprises and federations wanting to customize the distributed ledger for their needs. In MultiChain, the administrators, a group of trusted nodes within the federation, can dynamically alter permissions, with a consensus from other peers.

OpenChain [16] – OpenChain is a blockchain platform targeted for the enterprise, developed by Coinprism. Anyone can create an OpenChain instance easily. All aspects of the blockchain as well as rules that govern it are customizable and set at genesis by the administrator of the chain. The end users can then exchange assets over the chain.

BlockStack [17] – BlockStack is another platform that is targeted towards the enterprise. It allows for creation of private ledgers where internal assets can be moved between the enterprise users. It has quick settlement times and same security guarantees as provided by other blockchain platforms.

Chain [18] – Chain is another platform that lets companies create and deploy their own blockchains easily. The enterprise can target any market and deploy any type of asset. This is work in progress and should be available in the short term.

Sidechain/Anchored Chain Platforms

Sidechains are completely different blockchains that are connected via a two-way peg to the Bitcoin blockchain. The sidechain can convert Bitcoins to its native currency or work using Bitcoins. It can send Bitcoins back and forth between the sidechain and the main Bitcoin blockchain. Sidechains are built to allow completely new applications to have their own new applications completely independent of the Bitcoin network but allowing users who own Bitcoins to be able to start using the sidechains immediately with their Bitcoin address.

Anchored chain platforms on the other hand allow users to create their own blockchains suited for their application. To increase the security of the blockchain, the transactions within are organized in the form of a Merkle hash tree and the root hash is included in a widely used public blockchain, such as the Bitcoin blockchain. This increases the immutability of the anchored chain.

Platform	Blockchain Type	Blockchain Domain	Ledger Type	Source Code	API Support
SideChain Elements	Sidechain	Sidechains off the Bitcoin Blockchain	Public/Private	Open	✗
Factom	Anchored Chain	Generic recordkeeping Layer	Public/Private	Open	✓

Table 5: Sidechain platforms

Sidechain Elements [19] – Sidechain Elements from Blockstream is a platform for creating sidechains off the Bitcoin network. The sidechains that are created would be interoperable with the Bitcoin network. Currently, it is targeted towards research and development community to try out new applications. Not currently recommended for production grade applications. Blockstream's Liquid [21] is the first sidechain off the Bitcoin blockchain. Liquid improves the inter-settlement lag that Bitcoin transfers encounter while moving Bitcoins across accounts. These transactions are moved to the Liquid sidechain while still providing similar cryptographic guarantees.

Factom [20] – Factom builds a secure data layer that can be used for record-keeping and timestamping of any kind of data. It enables organizations to build their own blockchain depending on the use case. The application data is encrypted and hashed into the Bitcoin ledger from time to time increasing the security of the Factom ledger. Factom is used extensively to record and audit crucial pieces of information, such as land registries, government issued documents, etc.

Upcoming Platforms

There are several other platforms that are in their early offerings or are under development and would be available early to mid-2016. Notable ones to be analyzed in the near future would be InterLedger from Ripple [22], R3CEV's distributed ledger platform for banks and financial institutions [23], Blockchain-as-a-Service (BaaS) from Microsoft [24], Etherparty [25] and Linux Foundation's upcoming blockchain platform [26].

Use Cases

Below, we identify a few use cases that can utilize the power of blockchain technology and provide for powerful applications in the areas of E-Governance, healthcare and payments.

E-Governance – Empowering citizens

E-governance is a very prominent area where blockchain technologies can make a huge impact. The cryptographic guarantees, auditability and transparency that the blockchain possesses has the capability of adding a new dimension to E-governance. Below we discuss one such use case.

Consider a service where the government entity issues a certain card to its citizens – e.g. ration card, driver's license or a voting card. To apply for a new card with the government entity, the citizen has to show up in person with a filled application and supporting documents. After verification of documents, a new case is generated, which is to be processed within a certain number of business days. After that time period, the citizen can pick up the card from the government entity.

Above, we describe an ideal world scenario. In the real world, especially in developing countries, this process is seriously flawed and services are not delivered on time resulting in inefficient working, solicitation of bribes for providing service and frustrated citizens.

Blockchain technology can provide the needed auditing and transparency required in these scenarios. A blockchain enabled government service would work in the following fashion.

- To apply for a new card with the government entity, the citizen has to show up in person with a filled application and supporting documents.
- After generating a new case number to process the application, the information is submitted to the blockchain, where the issuing entity, and the case details along with the case number are timestamped and entered in an immutable ledger. This represents an OPEN transaction for that case.
- When the application is processed, the card is handed over to the citizen, and the case is closed, there would be a matching CLOSE transaction, which is now signed by two parties, the issuing entity and the citizen.
- An external auditing agency can look at the blockchain data and locate all OPEN transactions without a matching CLOSE transaction. Those are all the cases that are unprocessed that can be looked into and addressed to hold the responsible government authorities accountable in the real world.
- If the citizen is unhappy with the service or does not receive any, he has to power to not close the transaction, which reflects on the reputation of the government service.

Similar technique can be applied to improve customer service in any sector. Insurance is another area where such transparency will help tremendously.

Rural Banking

Implementing basic banking services on the blockchain should be very useful for catering to rural areas, who do not have banking services easily available. Rural banks can enable simple smartcards that allow rural area residents to use it as an enabler for a variety of functions, such as, making peer-to-peer payments, withdrawing cash, encashing loans, credit card, etc. All accounts and transactions can be recorded on the blockchain, thereby allowing other entities to interact with it directly. For example, government entities can lend money to eligible rural residents as per various government schemes. This money can be instantly credited and made available to individual customers. Allowing for peer-to-peer payment should eliminate their needs to withdraw cash from branches or ATMs that might not be conveniently located.

Patient Data Management

Patient data management is another important application of data management on the blockchain. Complete access to a patient's medical record is extremely important for the doctor to mete out appropriate treatment. Right now, the onus of providing the correct medical history falls on the patient, since the patient might be visiting different doctors and institutions for different ailments. These records are typically paper records that could get lost, misplaced or forgotten. There is a large percentage of the population that is completely unaware of the importance of providing appropriate medical history or is ignorant about it. Kids, elderly patients or immobilized patients in emergencies are not able to provide their medical history. Blockchain based medical history lookup can provide doctors and emergency responders with quick ability to look up patient's medical history and save patient's life in emergencies.

Every doctor/medical institution adds a case record to the patients file on the blockchain, which is timestamped and maintained on the blockchain, along with information about the doctor/institution himself. This provides an entire timeline of medical treatments received by the patient during his lifetime. Also, the patient cannot lie or hide medical conditions from the doctor.

Global Wallets

The idea of a global wallet is to enable businesses operating in multiple countries to be able to support their clientele with eWallet payments across its services in any country. Consider a transportation company UCab that allows users to get a taxi, private car or a ride share using a smart phone app, in multiple countries. Such services can benefit tremendously by providing seamless service to end users to pay via its eWallet in multiple countries. The eWallet can be integrated with a blockchain based foreign exchange conversion service like Ripple to provide instantaneous currency conversion of the amount required to pay for the ride. Consider the example where an UCab User A residing in the US is travelling to Japan for business. Below are the steps outlined on how his global UCab wallet would work.

- The user loads his UCab wallet with Y US dollars, which are debited from his US bank account. He estimates Y US dollars are enough to cover his expected number of taxi rides in Japan.

- He calls for a taxi in Japan using UCab. While paying, he asks for a currency conversion in Japanese yen. The wallet deducts the exact amount of dollars (according to the currency conversion rate for the day) equivalent to the amount of yen that was the cost of the taxi ride User A's UCab wallet.

This global wallet can be implemented by using a blockchain-based protocol for finance called Ripple initially developed by Ripple Labs (now Ripple). Ripple allows for real time cross currency settlement guaranteeing the lowest forex rate. By integrating this into the Wallet software, using Ripple APIs, real time cross currency exchange can be achieved.

Cross-currency micropayments

Smaller businesses that deal with international employees or international firms can benefit tremendously from instant cross currency payments. These businesses can benefit by using block chain based currency settlement networks and make instantaneous payments to other worldwide institutions in their native currency, without having to engage in expensive wire transfer charges, long delay for clearing and settlement, etc. These businesses can benefit from an elaborate front end built for them that can integrate with blockchain-based financial protocols, such as Ripple.

Conclusion

After a lot of initial hype about blockchain technologies, we now see some main players in the field in terms of platform offerings. The landscape is still changing very rapidly in terms of applications and platforms choices are not as easy to make with new ones are in the making and will likely be open-sourced in the short term. In this document, we present what is currently available and appear to be good choices when developing certain category of applications. We also present some use cases for blockchains that might be interesting to realize in the areas of E-governance, healthcare and payments.

References

[1] Colored Coins, http://coloredcoins.org/

[2] Coinprism, http://coinspark.org

[3] Coin Spark, http://coinspark.org

[4] ChromaWay, http://chromaway.com/

[5] Omni, http://www.omnilayer.org

[6] Ripple, https://ripple.com/

[7] HyperLedger, http://digitalasset.com/hyperledger/index.html

[8] Counterparty, http://counterparty.io/

[9] Stellar, https://www.stellar.org/

[10] BitShares, https://bitshares.org/

[11] Nxt, http://nxt.org/

[12] Ethereum, https://www.ethereum.org/

[13] Rootstock, http://www.rootstock.io/

[14] Codius, https://codius.org/

[15] Multichain, http://www.multichain.com/

[16] OpenChain, https://www.openchain.org/

[17] BlockStack, https://blockstack.io/

[18] Chain, https://chain.com/

[19] SideChain Elements, https://blockstream.com/

[20] Factom, http://factom.org/

[21] Liquid, https://blockstream.com/2015/10/12/introducing-liquid/

[22] InterLedger, http://interledger.org/

[23] R3CEV, http://r3cev.com/

[24] Microsoft'sBlockchain-as-a-Service (BaaS), (link)

[25] Etherparty, http://etherparty.io/

[26] Linux Foundation's Blockchain Platform, https://blockchain.linuxfoundation.org/

[27] Enhanced Padded Order based Coloring (EPOBC)

About Persistent Systems

Persistent Systems (BSE & NSE: PERSISTENT) is a global company specializing in software product and technology services. For over two decades, Persistent has consistently been selected as the trusted innovation partner for the world's largest technology brands, leading enterprises and pioneering start-ups. Persistent has a global team of more than 7,800 employees worldwide including offices and delivery centers in North America, Europe, and Asia. Persistent develops best-in-class solutions in key next-generation technology areas including Analytics, Big Data, Cloud Computing, Mobility and Social, for the independent software vendors (ISVs), telecommunications and media, life sciences and healthcare, and financial services verticals. For more information, please visit: www.persistent.com

India
Persistent Systems Limited
Bhageerath, 402,
Senapati Bapat Road
Pune 411016.
Tel: +91 (20) 2570 2000
Fax: +91 (20) 2567 8901

USA
Persistent Systems, Inc.
2055 Laurelwood Road, Suite 210
Santa Clara, CA 95054
Tel: +1 (408) 216 7010
Fax: +1 (408) 451 9177
Email: info@persistent.com