NextGen
INVENT CORP
think. invent. solve.

Blockchain Whitepaper for Startups

- By Blockchain Excellence Centre, NextGen Invent Corporation

NextGen Invent Corporation
sales@nextgeninvent.com
+1 508-753-1512

Contents

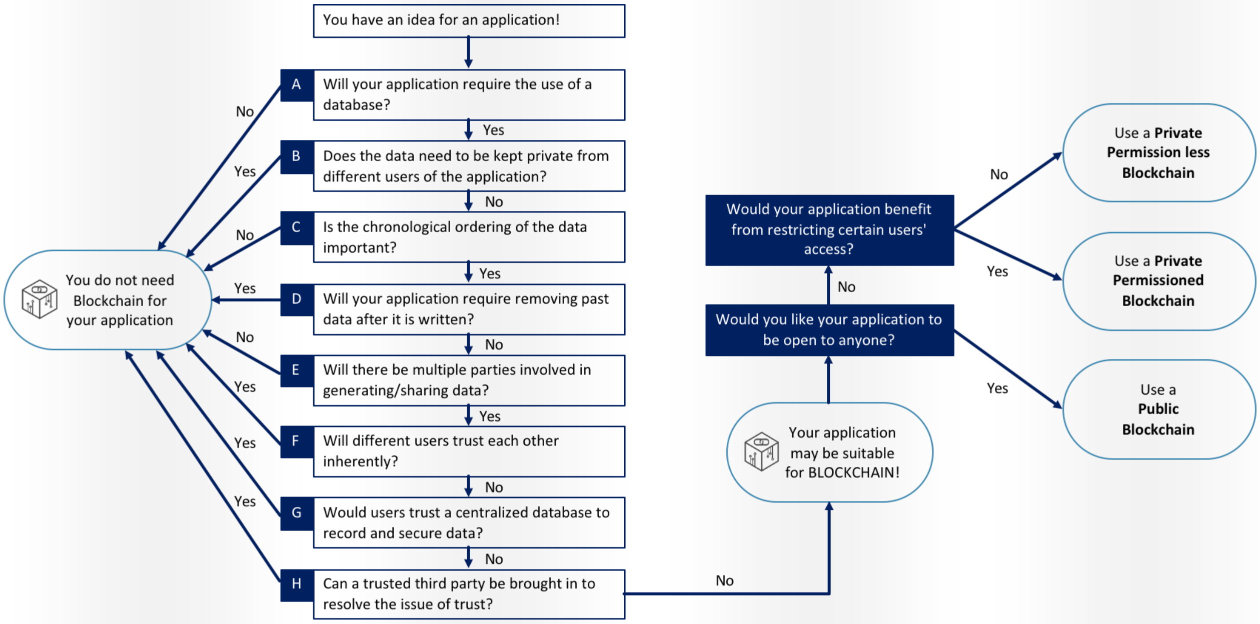
1 Introduction

Blockchain is a rapidly growing technology with disruptive solutions in multiple industries. The possibilities of blockchain technology are endless, as new use-cases for the technology are found every day. Entrepreneurs and executives are flocking to create the next big thing in blockchain. This white paper's purpose is to empower business executives in making better decisions related to decentralized applications (dApps or DApp) that utilize blockchain technology. Typically these applications piggyback off of existing blockchain frameworks like Ethereum.

In this paper, we will try to answer critical questions that are in business executives mind and highlight business signals and business strategies for the blockchain entrepreneur. Let's get started!

2 Criteria that makes an application a suitable candidate for the blockchain framework

Blockchain technology is not for all applications and use cases. The diagram below highlights the main question an entrepreneur should ask themselves to decide whether blockchain technology is the right technology for their application or not.


You have an idea for an application!
A Will your application require the use of a database?
B Does the data need to be kept private from different users of the application?
C Is the chronological ordering of the data important?
D Will your application require removing past data after it is written?
E Will there be multiple parties involved in generating/sharing data?
F Will different users trust each other inherently?
G Would users trust a centralized database to record and secure data?
H Can a trusted third party be brought in to resolve the issue of trust?
Yes
No
Yes
No
Yes
No
Yes
No
No
Yes
No
Yes
No
Yes
Yes
Yes
No
You do not need Blockchain for your application
Your application may be suitable for BLOCKCHAIN!
Would you like your application to be open to anyone?
No
Would your application benefit from restricting certain users' access?
No
Yes
Yes
Use a Private Permission less Blockchain
Use a Private Permissioned Blockchain
Use a Public Blockchain

a. Blockchain technology primarily deals with database-like data storage and recording.
b. Blockchain is a transparent data storage system. The data stored on blocks is accessible and visible to everyone (although identity may be kept secret). If data in your application needs to be kept private, don't use blockchain.
c. Blockchain keeps an ordered ledger of all chain activity. If the data recorded in your application does not need to be in chronological order, there may be a better solution for your project than blockchain technology.
d. Blockchain technology is mainly an immutable data recording device. If users of your application will want or need to change previously recorded information, blockchain may not be the best fit.
e. If transactions occur between two or more users of your application, or data is shared between users of your application, blockchain may be able to support your application and give it the peer-to-peer capabilities it needs
f. In the case that users trust each other inherently, blockchain technology would be of no use to your application. In fact, A database would be a better fit .Blockchain provides

mostly trustless interaction between users. If a centralized database cannot fix the issue of trust, then blockchain may be the answer.

g. If users of your application would not inherently trust each other or a central third party, then blockchain may be a good basis for your application.

3 What questions to get answered before starting a blockchain application?

3.1 What Value you are creating? Why can't the same value be created by a non-blockchain application?

Having determined that your application would be best implemented with blockchain technology, it is important to know why your application will be valued above a similar non-blockchain application?

For example:

In case of Title Insurance, blockchain brings trust, removes the intermediate firm role, and reduces the required time of the entire process. These benefits are tangible and add real value to a company's services.

3.2 Define the users of your application? (Companies? Individuals? Etc.)

It is important to know the market and whose problem(s) you are solving. The application should be designed in a way that your typical user can understand and navigate. Blockchain is a disruptive technology which means that the stakeholders will be different than those of a traditional app.

This question is greatly associated with the type of blockchain you may choose for your application. A public blockchain would allow your application to be used by anyone with connection to the internet and, in turn, would likely translate to the more individual users.

On the other hand, If you choose a private blockchain you would have to grant access to specific users.

3.3 What information will be stored in the blocks?

The information stored in the blocks will be defined by your business use cases. For example, A Bitcoin block contains all the necessary information to properly record a financial transaction between users. In a Bitcoin transaction, the wallet addresses of the sender and of the receiver are recorded as well as the amount of bitcoin sent between them and the timestamp of when the transaction was recorded.

It should be noted that Different blockchain platforms have limitations on the amount of data that can be store in a single block. Your application architecture will need to consider this.

3.4 What logic should be used in smart contracts?

Smart contracts are an effective way to automate transactions between users by setting up encoded agreements. An example of a smart contract is the agreement between Bob and Alice as described below.

Bob will give Alice $100 if the Patriots win the Super Bowl.

(if Patriots win, Bob = -$100 and Alice = +$100)

If, however, the Patriots lose the Super Bowl, Alice has agreed to give Bob $500.

(if Patriots lose, Bob = +$500, Alice = -$500)

A smart contract can represent the logic of this exchange agreement using code. The logic can be written into the blockchain, so that, as soon as the final whistle of the Super Bowl sounds, Bob's and Alice's accounts will be updated based on the outcome of the game.

3.5 What will the associated cryptocurrency be if there is one?

Cryptocurrencies are a way to incentivize activity on your blockchain application. Cryptocurrencies solve the problem of trust by ensuring that work must be done to get payment, and payment will only arise once the expected work is complete.

There are currently many cryptocurrencies keeping users and developers involved across different platforms:

Bitcoin (1 BTC = 6,000 USD) - Current Circulation: 17.15 Million BTC

Ethereum (1 ETH = 450 USD) - Current Circulation: 100.6 Million ETH

Ripple (1 XRP = 0.44 USD) - Current Circulation: 39,262 Million XRP

Bitcoin Cash (1 BCH = 700 USD) - Current Circulation: 17. 2 Million BCH

Litecoin (1 LTC = 77 USD) - Current Circulation: 57.4 Million LTC

Stellar (1 XLM = 0.2 USD) - Current Circulation: 18,766 Million XLM

Ethereum allows tokens to be kept in the Ethereum Wallet that are associated with decentralized Ethereum-based applications. These are specialized, project-based tokens called ERC-20.

3.6 What is the expected number of transactions the application will need to handle?

The precise number is difficult to figure out, but it is important to know what kind of performance to expect for the number of active users. If your application's utility can be used by many different people every day, expect a large number of transactions. Scalability will certainly be an issue to look out for; you'll have to ensure that your application performs well with large numbers of users. Knowing how many transactions will likely occur on your application will guide you to the best blockchain platform to build upon.

Ethereum, Stellar, and Hyperledger, while among very popular blockchain development platforms, each have their own limitations regarding capacity for traffic. Each of these numbers may vary depending on the hardware running the code, but the ballpark estimates for transactions per second of each of these platforms is:

Ethereum: ~15 transactions per second

Stellar: ~1,000 transactions per second

Hyperledger: ~3,0000 transactions per second

3.7 What is the cost of each transaction?

Blockchain transactions come at a cost. Each blockchain platform has its own transaction cost.For instance, microtransactions using Stellar would far better suit the application than Ethereum because of the relatively low transaction fees.

3.8 Who can see what information (Information access by role)?

Blockchain development typically follows a fairly transparent structure in which all users of a blockchain application can access information from anyone on the chain but cannot change that information. This is due to the information being stored publicly on the blockchain. A transaction on the Bitcoin blockchain, for example, would be publicly visible to all users of Bitcoin. However, anonymity is still ensured as partakers in transactions will be masked by their own unique hash addresses in the place of names. A recorded Bitcoin transaction shows the address of the sender, the address of the receiver, the amount of coins transferred, and the time of the transaction.

Note: Any information that needs to be recorded in a block but still needs to be private among a certain closed set of users can be encrypted using double and triple encryption, keeping it safe from unauthorized eyes. For more details, please send an email to deepak.mittal@nextgeninvent.com.

3.9 How would you like to raise the funds for your new Venture?

Not all projects can be self-funded by their founders. Few blockchain applications tend to rely on Initial Coin Offerings (ICO) for a good portion of their funding. For companies that are growing and in need of investors, an ICO can be an efficient way to boost their investment base. ICOs function as follows: a company will release their own cryptocurrency to the world in exchange for a more established crypto like Bitcoin or Ether. This puts their "coin" in circulation to begin accumulating value.

Note: Many ICO's end up failing now because the market is very dense but releasing an ICO can still be one of the best ways to get your company (and application) out into the view of the public as well as establish a strong basis of financial support. In the USA, ICO option is not available, so an entrepreneur has to choose smartly where will he/she will do ICO. Currently, expenses to do an ICO can range from $1M to $2M.

3.10 How will you analyze data?

It is always good to plan upfront on what information will be needed from the users of your application and how will you acquire that information in the simplest way. Navigating blocks to retrieve recorded information can be resource-intensive.

4 What are the technical and business challenges of blockchain application development?

4.1 Business Challenges

4.1.1 Financial

- Getting investors to be interested in your application can be a major challenge. Large investors will have teams of people making decisions based on everything your application has shown so far, but everyday people can also be investors. The problem with them is explaining how the technology works. A blockchain application, though it may be easy to use, is difficult to describe in everyday terms.

4.1.2 Marketing

- Marketing your application may pose a great challenge. There are different online tech news sources that could potentially help you market your product.
- Presenting a blockchain application to the consumer world brings its own challenge of vocabulary. There is a lot of new vernacular circulating around blockchain and its related concepts.

4.1.3 Risk

- Cryptocurrency markets tend to be very volatile, which can be a challenge for the business side of applications as investors may feel uneasy in the rising and falling market.

4.1.4 Legal

- New legislation and regulation is constantly being added to the public use of blockchain technology. It may be difficult to keep up with the quickly changing business and legal environment. Perhaps hiring a project team lawyer to help sift through newly published legal documents could be beneficial.

4.2 Technical Challenges

4.2.1 Development

- Finding a competent team of blockchain developers can be difficult in and of itself. Luckily it is a growing field of need. There is a growing demand for blockchain developers, which hopefully, will be met with some supply.
- Any blockchain application will require a high standard of technology and code to ensure that data is secure. This is vital to the performance of your blockchain application.

4.2.2 Platform/Environment

- Choosing the platform to develop upon can pose a serious challenge. Some blockchain platforms are friendlier to Dapp development than others. some use more common programming languages as their basis, making it easier to develop software.
- Security will always be a technical challenge that anyone trying to develop blockchain technology will have to face. With a distributed network of computers, it is difficult to see cyber-attacks much less attempt to stop them before they happen.

4.2.3 Testing

- Debugging the application software and getting it to operate smoothly on the countless number of different computer systems is a large technical challenge. Everyone has a slightly different operating system, making it difficult to create software that can fit whatever software/hardware it needs to integrate with.

5 Best ways to attract partners to use your blockchain app?

5.1 Release an ICO

An Initial Coin Offering (ICO) is a special fundraising strategy that helps build a base of investors and users for a new blockchain application. You can think of an ICO as an Initial Public Offering of a stock but for blockchain platforms. It gives people a chance to purchase some stock (in this case cryptocurrency or tokens) in a certain company (blockchain application), which acts as a sort of jump-start to that specific economy. After the release of an ICO, anyone with any amount of your blockchain application's specific token or currency will be personally invested in the success of your application and its economy.

Some blockchain platforms use their currency as a fuel for the execution of transactions and smart contracts. Ethereum's "gas" is essentially its cryptocurrency, ether, which compensates miners for performing computational work. If your blockchain application has real-life applications, there's a good chance your cryptocurrency will be more valuable as an asset.

The following chart lists 5 of the top ICOs of 2017:

ICO	Date	Total Raised (In Millions)	Description
FileCoin	September 2017	$257	FileCoin is a crypto based on a data capacity sharing blockchain. It allows users to "lend" their unused data to others for tokens.
Tezos	July 2017	$232	Tezos is an independent blockchain project. It is its own platform with dApp capabilities and smart contract capabilities.
Polkadot	October 2017	$145	Polkadot is a platform that connects various blockchains with different capabilities in order to transact across a multitude of chains.
Qash	November 2017	$106	Qash is a payment token for financial services on the LIQUID blockchain that provides additional liquidity by allowing trading to occur with different assets.
Kin	September 2017	$98	Kin is a custom crypto that is rewarded to the users of Kik, a messaging app. The tokens allow users

5.2 Stick to the issue at hand (Keep it Simple Stupid)

Simplify your Dapp to be user-friendly. Have a good interface for users to be able to easily utilize your Dapp's capabilities. Your goal is to maximize the number of people using the app and enjoying its benefits.

5.3 Allow room to grow

Designing your application as a base of development is always helpful to attract users.

Make sure it is clear to the users of the application that the application is constantly being improved. Working to optimize the software and improve upon what has already been implemented is one of the most important things to keep in mind. Ethereum, as an example, is a blockchain designed for improvement. The code is publicly accessible, and edits can be submitted by anyone with internet access. This allows users to contribute to the project's success and develop community around improving the project's performance. Ethereum also allows users to create their own decentralized applications on the Ethereum platform, which attracts developers as well.

5.4 Get the name out there

Reach out to tech or crypto news sources about your Dapp (the-blockchain.com, dappnews.io, etc.). Publish a whitepaper for your Dapp that explains the applications capabilities and methods. Getting your application’s name out into the tech world is the best way to build a base of miners/developers and keep on track to be the next big thing.

It can also help your cause greatly if you chose a blockchain platform to build on that has seen a lot of additional development. Investors and business partners want to know that the environment you are working in will allow you to succeed with your application. A history of development can be very beneficial.

6 Which KPI's is attractive to VCs?

Investing venture capitalists look for key performance indicators (KPIs) when selecting a blockchain application/company/project to invest in. Some of these KPIs are:

- **How big is the problem? And How your solution is disrupting market players and marketplace?**

  A blockchain solution is a large-scale business venture. Problems with a small number of afflicted population should not require a blockchain solution. Keep in mind other available applications and differentiate your project from those already in existence.

- **What value is created and for whom?**

  What advantage can your application give to its users that other projects have failed or neglected to produce?

- **What will be the customer acquisition cost?**

  How will you attract users to your application? Online news outlets and blockchain websites are a good way to publicize your blockchain project with little to no monetary investment. Find a high-traffic website of blockchain-interested users and spread the word about your new application.

- **Can a market leader replace the solution - risk analysis?**

  Keep in mind the risks associated with launching a blockchain project. Larger companies with greater resources can take an idea and adapt their own applications to fix something previously overlooked. Your application should solve a problem that larger companies cannot easily fix with their own established technologies.

- **Does the project have well-defined goals?**

  A project that is simply the implementation of a basic and specific idea will not be appealing for venture capital investors. They are looking for businesses that have a future goal in mind and a plan to work towards it for the next few years.

- **Has it been thoroughly tested?**

  Blockchain technology is very difficult and tedious to test. Making sure that it is operational and working without major flaws is key to showing investors that they can trust you with their money.

- **Can it be updated on the go?**

  Investors want to know that you can update your application or platform without much hassle (i.e. without shutting it down for a while and rebuilding it)

- **Is there developing talent to be able to sustain the market/product?**

  Investors like to know that there is a market for the kind of software development talent that is needed to work on the project. They want to know that there is room to develop more software on top of what is already in place, and they want to be assured that when problems in the code arise, there are people around who are available to help.

- **What are the risks involved in the projects blockchain ideas?**

  This question dives into the more technical questions about how difficult it would be for a blockchain to be attacked. It deals with cryptography, proof-of-work, and consensus protocols. Essentially, investors want to have a good picture of the major risks accompanying their investment into a specific project.

7 What are the different blockchain frameworks and which one should I use for my dApps?

With so many blockchains available in the age of constantly growing technology, it is common to ask why there are so many blockchain platforms and what the different capabilities of each are?

These are perhaps the biggest blockchains currently available for use and have certainly been under the spotlight as they develop new and improved capabilities and secure their chains.

7.1 Bitcoin

Bitcoin is by far the most commonly known blockchain because of its popularity in the media and because it's the first blockchain use-case. It is a distributed ledger that records financial transactions often with the use of its cryptocurrency (also called bitcoin or BTC). Bitcoin requires a computationally intensive mining process to add blocks to the chain.

Pros	Cons	Use Cases
• Sophisticated encryption mechanism • Proof-of-work algorithm as means of consensus • Digital signatures to verify transactions with public/private key encryption	• Block size limited to 1 MB • Scalability issues • Transactions not instant • High-energy mining process	• Bitcoin is the first case of a virtual wallet complete with a fully blockchain-associated currency, bitcoin • Sending/receiving money anonymously and with no need for trust

7.2 Ethereum

Ethereum is second to Bitcoin in its name's popularity. The Ethereum blockchain, similar to Bitcoin, has its own currency, ether (ETH). It is a platform that welcomes the development of decentralized apps, and the Ethereum wallet even has ERC-20 tokens which are a form of currency associated with specific applications or projects on the Ethereum blockchain.

Pros	Cons	Use Cases
• Popular platform for ICO; ERC-20 tokens	• Smart contracts are very touchy and cannot be easily edited or amended once they are in circulation • Legal issues concerning business between two parties are not fully dealt with by smart contracts and can require a third party legal consultant to develop ground rules	• Smart contracts for business • Legal contracts through the smart contract mechanism • Financial services

7.3 Ripple

Ripple is a blockchain that has been created to allow for large "clustered", cheap transactions between big companies. It has a native currency, XRP.

Pros	Cons	Use Cases
• Very high-speed transaction processing system (capable of 50,000 completed transactions per second) • Very little transaction fees • Integrated protection rules and protocols to detect illegal transactions and even suspicious activity reporting	• Blockchain is mostly controlled by Ripple Labs, not the most distributed or democratic platform • Prerequisites (requirements) for users to utilize Hyperledger capabilities (bad for small business users)	• Escrow contracts, which are contracts kept in the hands of a third party until a condition is met or a date is reached • Tipping services through different online platforms

7.4 Hyperledger

Hyperledger is an open-source blockchain platform with smart contract capabilities similar to that of Ethereum. It is mostly occupied with large-scale businesses and their associated transactions. Hyperledger, unlike many other blockchains, does not have its own associated currency.

Pros	Cons	Use Cases
• No mining • Friendly to big businesses • Allows creation of permissioned blockchains to ensure data security and private transactions • Cryptographic access key technology for permissioned blockchains	• Difficult to build on because of control of large companies and little room for the success of smaller business • IBM-like companies dominate the market	• Financial world, big bundled transactions between large companies • Healthcare, faster distribution of patient data • Supply-chain management, shipments and products can be tracked from their cultivation/production to sale

7.5 LISK

Lisk is a javascript-oriented dAPP development blockchain platform. It encourages the development of dAPPs and even hosts a dAPP directory to allow users to search for available dAPPs. Lisk has an associated cryptocurrency called LSK.

Pros	Cons	Use Cases
• dAPP development is big plus, all in Javascript which removes the ambiguity of programming language choice • Very little overhead regulation on dAPP development and no fees	• Can have significant delays in mining process if blocks are unable to be found	• Endless possibilities in use cases because of dAPP development opportunity

7.6 Stellar

Stellar is a blockchain that allows simple smart contracts. It is not the most dAPP friendly because of its non-Turing complete computing environment, meaning it does not have the same computational abilities as, say, Ethereum would.

Pros	Cons	Use Cases
• Simple smart contracts make simple agreements easy to implement	• Public chain, everyone can see everyone else's transactions	• micropayments, as transaction fees are low

As you can see there are many blockchain frameworks, some with dAPP capabilities and others without. Each framework has its specific advantages and drawbacks, but clearly each serves a given purpose in the real world using blockchain technology.

7.7 Which blockchain framework is best for which use cases?

Our suggestion to entrepreneurs is to choose the blockchain platform based on three main criteria: a) Which blockchain has the most similar use cases implemented? b) Are you planning to raise funds for your dApps using ICO? c) Is your strategic partners, have their dApps in the same blockchain framework or not.

Requirements	LISK	Stellar	Ethereum	Hyperledger	Ripple	Bitcoin
Would you like the platform you chose to be developer-friendly instead of having only predefined transactions and contracts?	✓	✓	✓	✗	✗	✗
Is scalability a necessity for your application? (Do you expect very high levels of activity?)	✓	✓	✗	✓	✓	✗
Would your application benefit from a native cryptocurrency from the platform it operates on?	✓	✓	✓	✗	✓	✓
Would your application better serve its purpose with its own customized mini-blockchain?	✓	✗	✓	✗	✗	✗
Is speed of transactions an important part of your application's utility?	✓	✓	✗	✓	✓	✗

7.8 How to calculate Gas for each blockchain framework?

Many blockchain frameworks have some type of “gas” or payment for running programs or completing transactions on their platform. Ethereum is of the most popular blockchain platforms and its gas system is typical of how other blockchains might operate as well.

Ethereum gas is a compensation for computational effort. Changing the state of the Ethereum blockchain requires work completed ultimately by the network of nodes. Gas on the Ethereum blockchain is associated with a transaction or smart contract. The instigator of a transaction pays the miner for executing their smart contract, but they must define their own price. If the price they chose is too low, miners will hold off on executing their transaction until other more profitable transactions are complete.

The amount of gas required for each transaction depends on a few things:

1) Was there a smart contract involved? If so, how complex is that contract? (How much computation is required?)
2) How much data is stored in the blocks for each transaction?

Each of these two things require a certain amount of computational energy and therefore a payment for their completion.

"Gas" is a mainly Ethereum-based concept. On the Ethereum blockchain smart contracts can execute code resulting in some sort of transaction. This code can be broken down into discrete steps (adding two numbers, comparing two values, checking an account balance, etc.) each of which requires a certain amount of "gas" to complete.

For example:

Let’s assume Harry and Sally have an agreement which is encoded in a smart contract on the Ethereum blockchain. They have agreed that on January 1st of the next year (2019) whoever has more Ether in their account will get 100 Ether from the other. Ignoring timing for the sake of simplicity, the contract code can be broken down into these pseudo-steps:

1) Check Harry's account balance. (CheckBalance = gas price of checking any account's wallet balance)
2) Check Sally's account balance. (CheckBalance)
3) Compare the two resulting balances. (CompareValues = gas price of comparing two numerical values)
4) Credit 100 Ether to the lesser account. (CreditAccount = gas price of adding Ether to a wallet)
5) Subtract 100 Ether from the greater account. (SettleAccount = gas price of removing Ether from a wallet)

Each of the operations described above would have a specific gas price associated with them making the total gas price for running the contract a value reached by this equation:

CheckBalance×2 + CompareValues + CreditAccount + SettleAccount = gas price

(units of GAS) 20×2 + 3 + 2,100 = 2,143

(CreditAccount and SettleAccount are combined in transfer function with gas limit 2,100)

The suggested gas price of this contract would be 2,143, which is approximately 0.000002143 ETH or $0.01. This simple of a contract is comparable to a simple transaction, resulting in a very inexpensive agreement. Contracts can quickly gain complexity and start to require much more gas for their execution.

On the Bitcoin blockchain there are fees associated with every transaction. The minimum fee you would have to pay for a transaction to be completed (included in a block) is the 6 blocks fee, meaning that your transaction would be included sometime within the next six blocks. The current six-block fee is $0.07 per transaction. The current next-block fee (asap recording of transaction on the blockchain) is $0.26 per transaction. This is different than Ethereum's concept of gas, but it essentially shows that operating on blockchain technology requires some sort of payment for the collective computing power that is utilized.

On other platforms a simple transaction is also accompanied by a running fee. Some call the fee "gas", but this term is often used to describe Ethereum only.

Here's how much a simple transaction (sending money from A to B) costs on different platforms.

Ripple: 0.00001 XRP (0.00 USD)

Lisk: 0.1 LSK (0.49 USD)

Stellar: 0.00002 XLM (0.00 USD)

In the case of Ripple and Stellar, the transactions are not entirely free, but the simplest transactions (those that require no computation) are the cheapest. Stellar and Ripple are also two of the least expensive blockchains on the market. The numbers above reflect minimum fees for any transaction.

Computational work spent in the execution of smart contracts is paid for in gas. This is an incentive for miners to be able to run complex code as well as for the users of smart contracts to simplify them to save money on transaction costs, ultimately resulting in a blockchain-wise

Additionally, since the price of gas is determined by the user, if any transaction or money transfer needs to be completed quickly, that user can simply set their price of gas to be slightly higher than the average across the blockchain, thus providing miners with incentive to complete their transaction first.

As a user it is important to keep in mind that transactions can “run out of gas”. This happens when the user sets a predefined gas limit on their transaction or smart contract. If the amount of gas required is above the maximum limit set by the user, execution of their contract or transaction will fail and they will lose whatever ether was already spent.

Other platforms like NEO and Qtum have a gas currency, which is either a subset of their own crypto or, like in the case of NEO, an entirely separate cryptocurrency altogether. NEO’s is called GAS. Regardless of the name or type of currency, all blockchain gas operates fairly similarly to Ethereum.

8 Top 5 ways to make secure transaction and data in a blockchain app?

8.1 How to secure transaction and data in a blockchain app?

The security of data in any blockchain platform is a key issue in development . Typically, blockchain frameworks will allow users to have a private key which, when paired with their public key can quickly verify the legitimacy of a user and the information they are putting forward. This encryption method is used to ensure that users (perhaps with destructive motives) cannot alter transactions and data that has already been stored on the blockchain. A private key act as a sort of digital signature to show that a transaction is legitimate.

Encryption mechanisms also play into the consensus protocols of a blockchain platform. Consensus protocols are a defined set of rules by which data and transactions must be verified so they can be included in the data on a block. This verification has a few common variations: Proof of work (Bitcoin), Proof of stake (Ethereum), and Proof of elapsed time (Hyperledger). These different protocols work similarly to ensure data integrity across all blocks in the chain.

Once written to the block, data cannot be changed. The only way data can be erased is if a forked chain (this occurs when two new blocks are found at once) becomes longer than the original. For this reason, some blockchains recommend waiting for the verification of a few subsequent blocks before considering a transaction final.

8.2 Securing a blockchain app: 5 steps

8.2.1 Define regular user permission

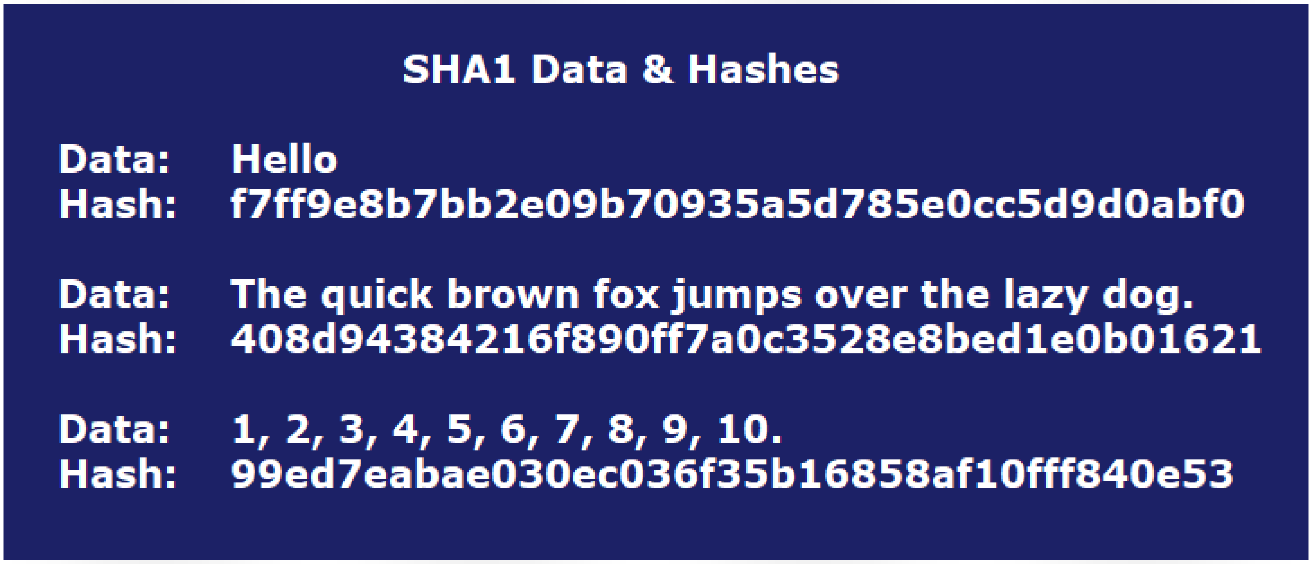
It is important to establish read accessibility protocols for the general user. Bitcoin allows all users to see a collective transaction history for the entire blockchain, but your application may deal with more on-chain data than simply transaction histories. Since the data on the chain will be accessible to all users, be sure to define the types of data that will be written to the blocks and ensure that its accessibility will not hinder or harm any individual users of the application.

8.2.2 Have a consensus mechanism

- A consensus mechanism ensures that the data written to the blocks in the chain associated with your application is valid. It is a way to prevent fake transactions and false on-chain data.
- The three most common mechanisms are Proof of Work (Bitcoin), Proof of Stake (Ethereum), and Proof of Importance (NEM).
  - PoW: miners verify written transactions on the blockchain and do not finalize them until other blocks have been added past those in question.
  - PoS: users' coin stake determines their likelihood for mining the next block. A user with %50 of all coins on the chain would have a %50 chance of receiving each new mined coin.
  - PoI: productive network activity (mining, writing, verifying, etc.) is rewarded as a measure of importance to the chain, which then operates like PoS.

8.2.3 Utilize cryptography

Hashing, a method of data encryption, allows any piece of data or information to be converted into a unique and random string of text. A hash is an example of an easy one-way verification. A phrase (perhaps a username or password) can be hashed, encrypting the phrase itself and protecting its owner's privacy. This hash can then be repeatedly verified by the same user by running their data through the hashing function . Because the functions will always output the same hash for a given string, the user's identity can be easily verified while still being cryptographically protected.



SHA1 Data & Hashes

Data: Hello
Hash: f7ff9e8b7bb2e09b70935a5d785e0cc5d9d0abf0

Data: The quick brown fox jumps over the lazy dog.
Hash: 408d94384216f890ff7a0c3528e8bed1e0b01621

Data: 1, 2, 3, 4, 5, 6, 7, 8, 9, 10.
Hash: 99ed7eabae030ec036f35b16858af10fff840e53

Common hashing mechanisms include SHA1, SHA-256, and MD5 each of which perform the same overall function (encrypt data) but with different methods.

8.2.4 Have transactions signed by participating parties

Cryptographic signatures on all transactions will ensure that transactions cannot be forced or faked. Any transaction that will be recorded should be signed by all participating parties. This will verify the validity of the transaction.

8.2.5 Constantly debug and improve code

It is always important to keep on top of the code to make sure that improvements are being made and bugs can be found quickly.

9 Top 10 items of a blockchain app testing checklist?

Blockchain-based applications require extensive testing to ensure that all their complicated parts run smoothly. This is a difficult goal to reach since blockchain applications are run on a variety of different operating systems, each of which behaves slightly different from the rest. For this reason, however, testing is a crucial step to the development of decentralized blockchain applications.

There are different steps in the testing process, each of which attempts to stress individual aspects of the blockchain application. These steps are fairly standard and are usually applied in the testing of non-blockchain applications as well:

1) **Block size:** Ensure that the block size (amount of data) you have chosen for your individual blocks is consistent and based in code. Bitcoin has a block size of 1MB which is a hard-coded limit.
2) **Chain size**: Most blockchains have an unlimited chain size (more blocks can always be added). Make sure your platform or application is capable of this.
3) **Write**: Once you have set up your platform, use example data sets to test writing to the blocks in the chain. This ensures that the blockchain is operable on a basic level.
4) **Read**: Once you have tested the platform/application's writing ability to the chain, ensure that the information is accessible to users. This may entail creating separate users and attempting to access information stored on the chain.
5) **Transmission of data**: It is important to make sure that the block is consistent among different users. The data in the blockchain must be updated to every user once a transaction or data is written to the block. All reads from the block must be consistent throughout the network of users.
6) **Cryptography**: Test the cryptographical functions of your application, including generating public/private keys to ensure that the data in your blockchain is secure and encrypted.
7) **Security**: With different levels of security in blockchain applications, it is important to make sure that there is no interference between security protocols. Testing the security of a blockchain platform can mean deciding to change the consensus protocols.
8) **User load**: Testing performance and load can be done by stress tests. Have a sufficient number of generated users make arbitrary transactions and see how the blockchain handles the load. This testing will help expose any serious issues with performance and concurrency.
9) **Transaction load**: Have generated users make numerous transactions in a small amount of time to test the throughput. Current numbers for transactions per second are not very high (Bitcoin can only handle about seven transactions per second).
10) **Beta testing**: Release an official beta "preview" of your application with a limit to the number of users. This will allow your application to face real-world scenarios, possibly exposing any bugs or loopholes in the code that you may have previously missed.

Depending on your choice of blockchain platform, there are several available software for testing Dapps. Ethereum has an Ethereum tester that provides developers with necessary tools for testing their Ethereum-based application. Hyperledger provides Hyperledger Composer to test applications. These testing suites exist for several different blockchain platforms and allow developers to test their applications with as little extra effort as possible.

10 Consensus on the blockchain

Consensus is often a very complicated process by which blockchains can agree on data that they store. The common consensus protocols are Proof of Stake (PoS), Proof of Work (PoW), and Delegated Proof of Stake (DPoS). Here is how they differ:

If Alice sends Bob $1 (for the sake of example I will be using dollars instead of a specific cryptocurrency) on Bitcoin (PoW), Ethereum (PoS), and Lisk (DPoS), each blockchain will validate and store that transaction differently.

- PoW (Bitcoin)
    - Nodes of the Bitcoin network verify transactions as miners solve difficult cryptographic puzzles. This puzzle is associated with the blocks and each new block creates a space to append another. PoW assumes that most miners will work on the correct “chain” of blocks. The right chain will grow the longest the fastest. Essentially the blockchain is safe if 50% of work being put in by miners is honest. A new block is mined which includes Alice and Bob's transaction.

- PoS (Ethereum)
    - PoS differs from PoW in that it takes into account the amount of the blockchain’s cryptocurrency that each node has. The more coins a staker has, the more likely they will be the ones allowed to add a new block to the chain. This works best for blockchains with a set amount of coins. A block is created by the selection of a node from the pool based on their account balance. Then Alice and Bob’s transaction is written to the block. Token holders then vote on the validity of transactions.

- DPoS (Lisk)
    - Tokenholders vote for a delegate (or group of delegates) to verify the transactions for the whole chain. After a delegate is chosen they have power to verify transactions and collect rewards. This alleviates the pressure on regular nodes to keep working and allows a select group of people to validate the chain and keep the data true. After a delegate is chosen he/she votes to append Alice and Bob's transaction to the chain.