DZone
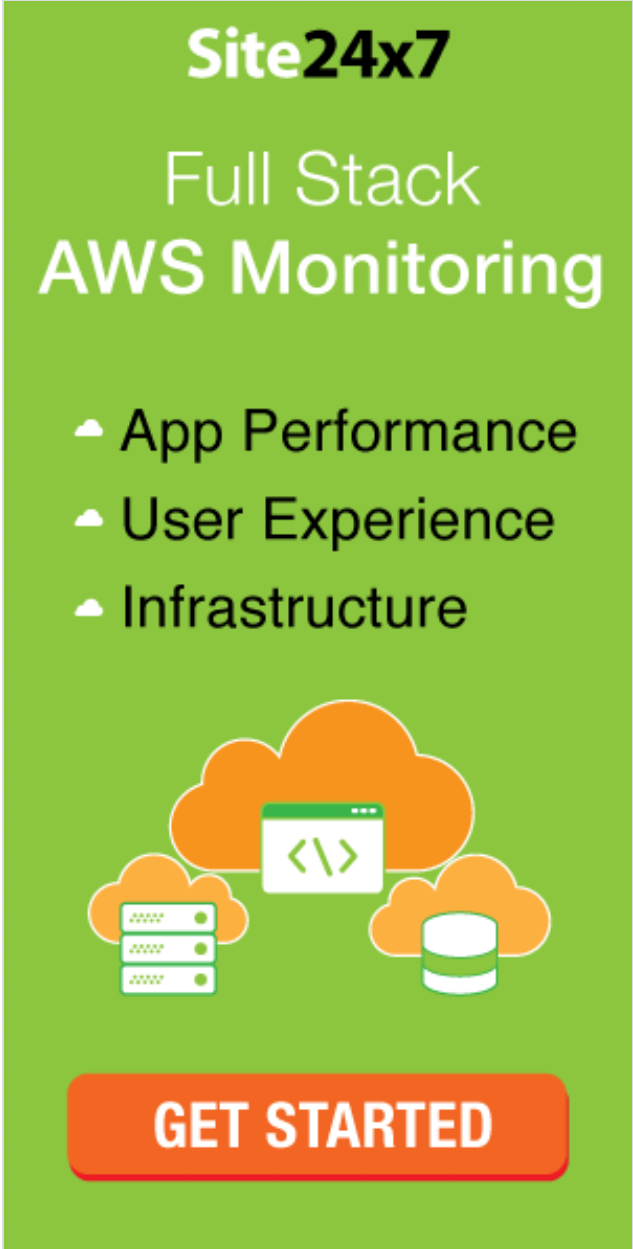
Discover the 6 Most Common Performance Testing Mistakes in the 2018 Guide to Performance

Download Guide ▸

The Bitcoin Protocol: How It Works

Learn the ins and outs of the world's most popular virtual currency, including how Bitcoin and blockchain work together and how Bitcoins are created.

by Samar Kishor · Jan. 11, 17 · Cloud Zone · Tutorial

Discover the all-in-one cloud to help teams build better software. Brought to you in partnership with DigitalOcean

Bitcoin is a form of digital cash that allows online payments between the buyer and the seller. It works as a digital ledger that records transactions and balances of accounts.

Bitcoins are exchanged using the Bitcoin Protocol built over the principles of cryptography. The protocol defines the procedure that is followed by a Bitcoin transaction from its creation, through validation and final confirmation.
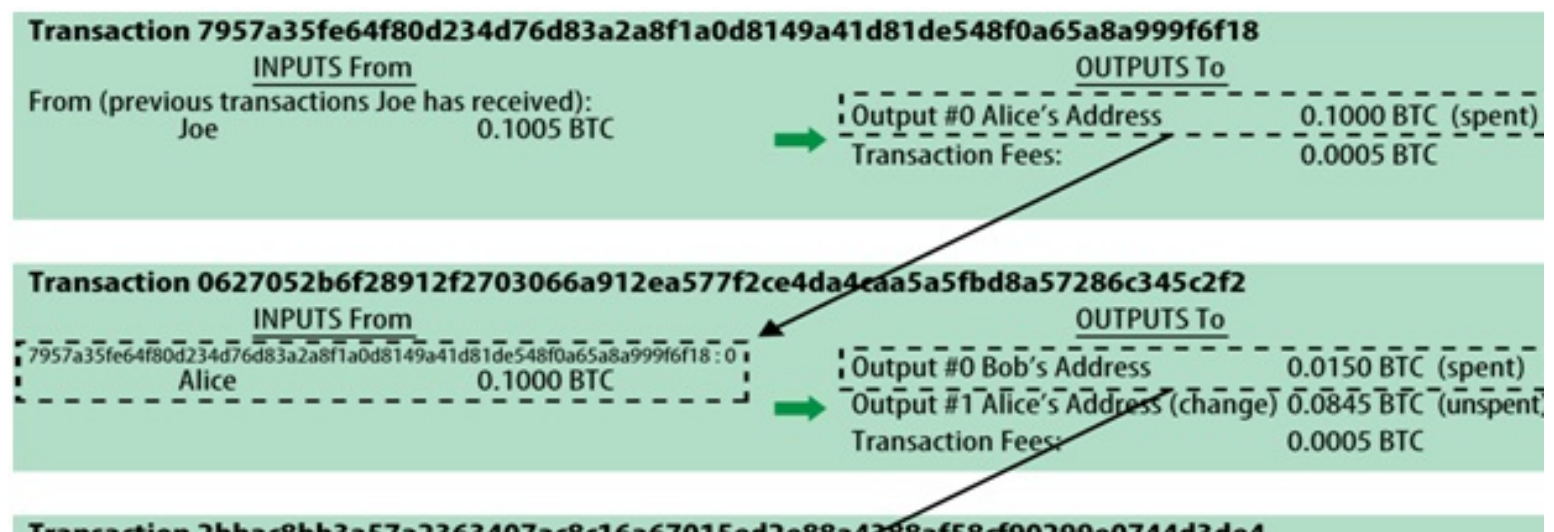
At the core of protocol is the Bitcoin transaction mechanism. Bitcoins are spent from electronic Bitcoin Wallets and are exchanged using Bitcoin transactions. In order to understand the protocol, let us first try to understand a transaction, the information it contains and how this information is processed.

Bitcoin Transactions

A Bitcoin transaction essentially contains the following information:

- ID: Unique transaction ID which is the SHA256 double-hash of the transaction data.
- Input: The bitcoin addresses that identify the sources of the bitcoins to be transferred. These are usually a previous transaction's output and are used to verify the sender and check the available balance.
- Amount: The number of bitcoins to be transferred.
- Output: The receiver's bitcoin address. In cases where there is leftover bitcoin change, the output should also include an entry for the sender's address to send it back, to be collected as "Transaction Fee" or to be sent to another receiver.

Outputs from one transaction can be used as inputs for another transaction. This creates a chain of ownership as the bitcoin value is moved from address to address.
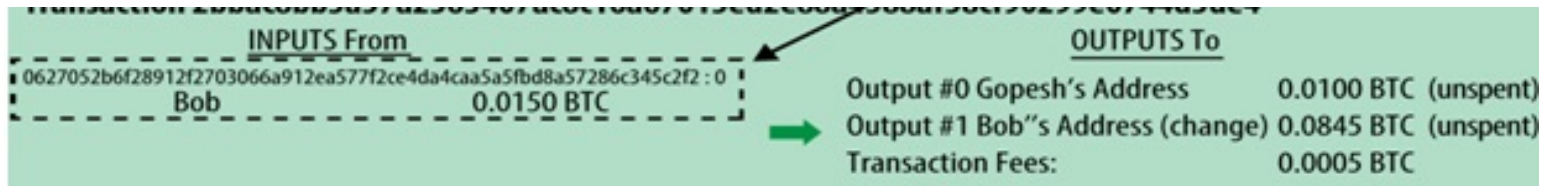
INPUTS From		OUTPUTS To	
0627052b6f28912f2703066a912ea577f2ce4da4caa5a5fbd8a57286c345c2f2 : 0		Output #0 Gopesh's Address	0.0100 BTC (unspent)
Bob	0.0150 BTC	Output #1 Bob''s Address (change)	0.0845 BTC (unspent)
		Transaction Fees:	0.0005 BTC

Figure 1: Bitcoin Transaction Chain

Transaction Validation

All digital cash transactions also need to be checked and verified for authenticity, duplicity, and cash availability. The validation of the transactions is not centralized and all participating nodes are authorized for it.

A Bitcoin Wallet account that initiates a payment transaction is identified by a Bitcoin address and a pair of public and private keys. To enable verification of the sender identity, transactions are digitally signed using the sender's private key and validated using his public key that is available to all the nodes.

The Bitcoin system orders the transactions into lists called *blocks*. These are subsequently linked to form a *blockchain*, a shared public ledger of all confirmed transactions. Transactions not yet included in the blockchain are unconfirmed and reversible.

The miners confirm and write these transactions into the blockchain. To prevent double-spending, a transaction is not marked confirmed until it has received a certain number of confirmations.

Each bitcoin mining node keeps a personal copy of the BlockChain which is updated whenever a new transaction arrives. This article explained that GPU is also a very efficient tool for the speedy mining of bitcoins. Subsequently, it also tries to validate the current and previous transactions in the block by solving a mathematical puzzle called the *Proof of Work*. The successful node that solves the puzzle gets a Bitcoin reward and its BlockChain approved and accepted by all nodes.

The Bitcoin Protocol

In terms of the transaction creation and validation process, the Bitcoin Protocol can be stated as below:

- A new transaction is broadcast to all participating nodes in the network.
- Each node collects new transactions into a block.
- Each node tries to validate the new transaction and all previous ones by finding a solution to the Proof of Work for the block.
- The node which finds the solution broadcasts the solved block to the network.
- Nodes validate the transactions in the block and accept the block.

- Nodes start working on the next block. A hash of the last accepted block is created and used as a reference in the next block.

Summary

The Bitcoin protocol is based on collaboratively maintaining the Bitcoin ledger. The digital cash is transferred through transactions which are confirmed only after validation of key criteria and joint consensus by participating nodes through a mathematical puzzle based voting process.

Balance virtual machines with a healthy amount of memory tuned to host and scale applications. Brought to you in partnership with DigitalOcean

Like This Article? Read More From DZone

An Introduction to Ethereum and Smart Contracts: Bitcoin and the Blockchain

What Is the Real Value of Using Cryptocurrencies?

Blockchain Security Theory and the Cryptocurrency Boom, Part 1: Theory

Free DZone Refcard
Getting Started With Kubernetes

Topics: BITCOIN , CLOUD , BLOCKCHAIN , CRYPTOCURRENCY , TUTORIAL

Opinions expressed by DZone contributors are their own.

SUBSCRIBE

Get the best of Cloud in your inbox.

Stay updated with DZone's bi-weekly Cloud Newsletter. SEE AN EXAMPLE

Cloud Partner Resources

Build, Deploy and Scale Cloud Applications Faster and More Efficiently
DigitalOcean
↗

Whitepaper: Site24x7: Powerful, Agile, Cost-Effective IT Management from the Cloud
Zoho
↗

Build, ship, and run distributed applications with Docker
DigitalOcean
↗

One-click install and deploy Node.js to a SSD cloud server in 55 seconds
DigitalOcean
↗

4 Metrics to Monitor When Scaling Up and Down in the Cloud

If we aren't going to do computing the same way we used to, we can't monitor how we used to either. Get the latest on cloud monitoring here.

by John Julien ⋇ MVB · **Apr 13, 18** · **Cloud Zone** · **Tutorial**

Site24x7 - Full stack It Infrastructure Monitoring from the cloud. Sign up for free trial.

Fans of *Star Trek: The Original Series* know that The Enterprise was not capable of going past Warp Factor 8 for long periods of time. That would be all the power Scotty could give the starship before it started breaking up.

The same thing is true with traditional on-premise computing: the hardware has limitations on processing power and storage. With cloud computing, however, these limitations virtually disappear. Cloud computing is allowing companies to recognize the benefits of scalability in ways no one ever imagined.

Picture a scenario where your company needs more processing power. Traditional configurations would require you to plan, purchase, and allocate those resources, which could take weeks or even months. By then, the requirements may have already changed. Some companies even purchase for future scaling, which causes them to spend before they need it.

Cloud computing releases that burden of knowing how much processing power will be needed in the future. You simply ask for more (or have your configuration ask for you, triggering resources when it needs more power).

Due to its highly scalable nature, monitoring cloud computing is very different from monitoring on-premise servers. The cloud vendor may have tools you can use. However, if they fall short of your monitoring requirements, you need to seek alternative solutions. In this article, you will discover the metrics to track and how to select the right monitoring tools for your situation.

What Metrics Should You Track?

There's a vast number of metrics regarding cloud services that could overwhelm your organization. Therefore, you need to determine which metrics are the most important to track and find the tools that will report those metrics.

Obviously, your needs will be different from other organizations and perhaps even other departments. However, some common metrics should serve as a baseline for your monitoring activities:

Security

This deals with both internal and external security. You will need to find out from your security team which metrics to track. This may require an audit of the cloud monitoring tools to ensure everything on their checklist is met.

One slippery issue with security and cloud applications is that it's relatively easy to add new users to an application. While that is mostly a positive development, from a security perspective, not every user should be allowed access without going through proper security protocols.

New application offerings from cloud vendors could cause backdoor access to other systems if the vendors are not vigilant in preventing this from happening. The security is at the mercy of the cloud vendors. Cloud monitoring tools should be capable of detecting these breaches. When you discover such breaches, the cloud vendors should make them a priority to fix.

Performance

While this covers several layers, determining where bottlenecks are happening in your applications is essential. In many cases, cloud vendors provide a minimum acceptable level of performance, which might not be enough when you want to improve the performance of your applications. Luckily, competition for cloud services continues to heat up. This is forcing vendors to pay more attention to the performance of its applications.

One best practice when monitoring performance is to view all the metrics in one central location. Otherwise, you will have to constantly cut-and-paste information to match up your metrics. Further, when dealing with hybrid cloud solutions, the monitoring tools must adjust to give reliable reports. Automating as much of this as possible is smart.

Costs

In general, you should save money when adopting cloud technologies, but that doesn't mean you are free to spend like it's an open checkbook. When you allocate more resources on the cloud, you can expect this to cost more money. How much more will depend upon the agreements you have with your cloud vendors and what functions you want to include. One of the best ways to manage costs is to

monitor the usage of your resources. Scale back any resources that are deemed unnecessary or don't meet the objectives of the business.

Uptime

If certain aspects of your architecture are failing, you want to know this as quickly as possible. You'll need a tool that gives detailed information about this will help get to the bottom of the situation quickly. Your tool should also help determine the frequency of failures.

Knowing which metrics to track helps you make better decisions for your architecture. Conversely, vanity metrics could lead you to make the wrong decisions. Try to focus on the metrics that affect important aspects of your system. The above four factors (security, performance, cost, and uptime) are good places to start when doing an audit of your metrics. Remember, you aren't locked in. Add or subtract different metrics as your needs and applications change.

Finding the Right Tools

To determine specific metrics to monitor, start with the ones you were tracking before your decision to switch to the cloud. Then, look for cloud monitoring tools that will report as many of those metrics as possible. If the tools don't report every metric on your list, you will have to let the less important ones go. Vendors are adding features all the time. Ask potential vendors how frequently they add new features and whether customers have a say in the process.

When you have a solid understanding of your essential metrics, you should learn what features cloud monitoring tools will provide that will match your criteria. There is some give-and-take. However, your requirements will change, and you'll revisit the ones you dropped.

I hope you have a better grasp of what is needed to select monitoring tools for your cloud solution. Determine what metrics are important for your organization and seek out vendors who offer solutions that come close to providing those metrics.

Site24x7 - Full stack It Infrastructure Monitoring from the cloud. Sign up for free trial.

Like This Article? Read More From DZone

Monitoring Tools for Serverless Environments and AWS Lambda

Avoid APM Vanity Metrics - Use What Matters

5 Public Cloud Monitoring Challenges You Need to Overcome

Free DZone Refcard
Getting Started With Kubernetes

Topics: CLOUD, CLOUD PERFORMANCE, CLOUD MONITORING, PERFORMANCE METRICS, CLOUD SECURITY, COST ANALYSIS, CLOUD VENDORS

Published at DZone with permission of John Julien , DZone MVB. See the original article here. ↗
Opinions expressed by DZone contributors are their own.