SPARKL®

Leverage Blockchain for Assurance

How SPARKL® technology makes blockchain work for the Internet of Things

Solution Brief

Inside This Brief

About SPARKL®

All enterprises suffer from the black box swamp. Systems that work fine on their own, but won't play nicely with others.

It's hard to describe how a system should work - let alone how or why different systems interact.

SPARKL® is powerful technology for managing the behaviour of distributed systems.

The simple, declarative Clear Box® modelling language lets you express the behaviour of all your systems - from applications right down to network infrastructure.

Then, the lightning fast, distributed SPARKL Sequencing Engine uses Clear Box to make them work together - driving events between all your machines, applications and things.

It provides Distributed Intelligence for true fog computing, allowing edge devices to interact with or without the cloud.

It introduces Reasoned Provisioning which spins up secure, on-demand infrastructure to meet the need of actual business logic.

SPARKL leverages standard distributed ledger technology to log every event between your systems in a tamper-proof Audit Trail to solve compliance and regulatory reporting across machines and systems, old and new.

SPARKL designs and develops the SPARKL® Sequencing Engine in London, UK. We work with partners including Cisco and Intel to market the product to innovators and customers worldwide.

SPARKL.COM

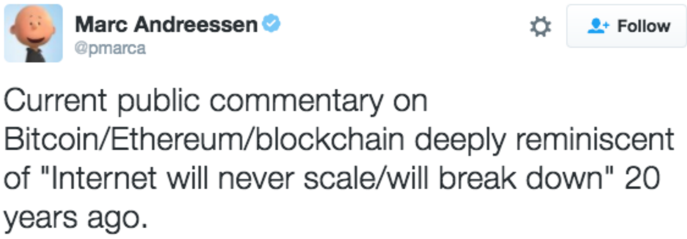
The Rise of Blockchain

After revelations that the NSA and GCHQ are carrying out mass surveillance around the globe, Sir Tim Berners-Lee, the man who forever changed the course of global communications, is now asking for an Internet that is open and transparent for all, free from government control and corporate regulation.

What might happen, Sir Tim asked, if we harnessed new technologies to help create a more decentralised web? Blockchains, the underlying technology behind bitcoin, could help realise this dream.

At first, blockchain technology was primarily for and by anti-establishment figures — for example, the now-defunct Silk Road operators — seeking independence form centralised control (and to keep their Bitcoin safe!).

But money is one application of many, with a variety of use cases cropping up across various industries.


Marc Andreessen
@pmarca

Current public commentary on Bitcoin/Ethereum/blockchain deeply reminiscent of "Internet will never scale/will break down" 20 years ago.

At a blockchain conference in early 2016, a Fedex manager complained about the company's supply chain problems. "***It would be nice if someone could leverage blockchain tech to prove that a package did actually make it to the final destination, with something other than an illegible signature.***"

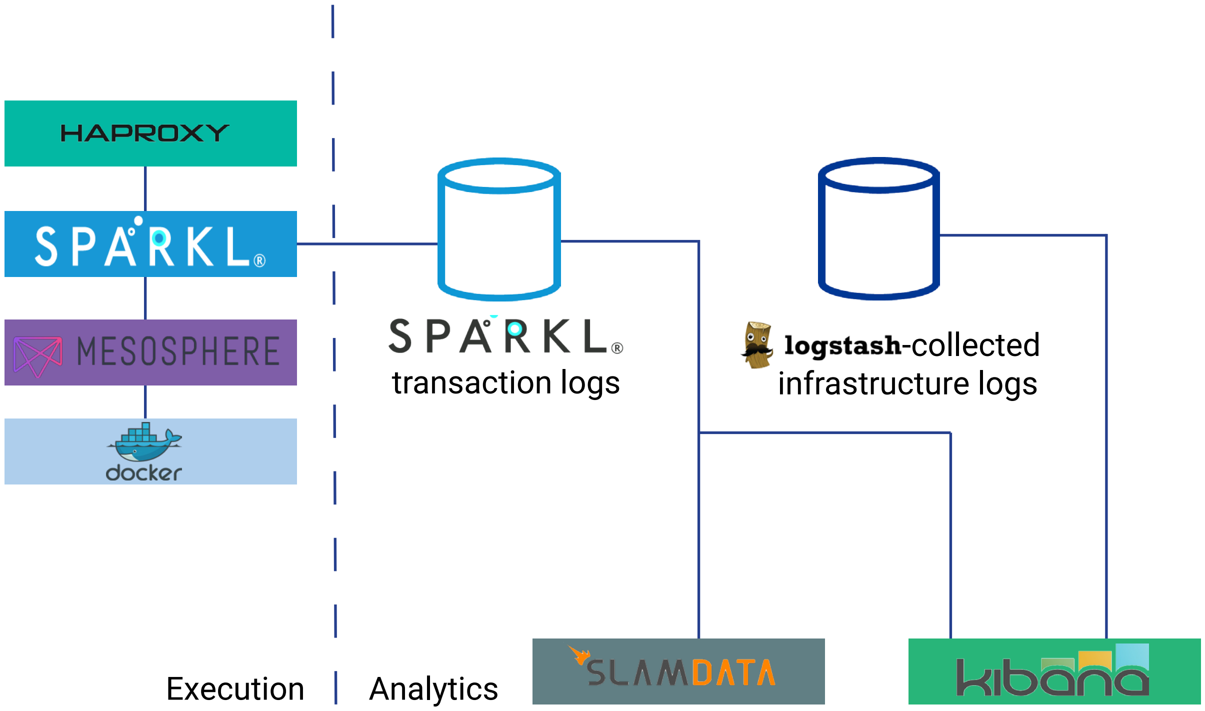
Given the decline of public trust in governments and banks, assuring customers of true data provenance could be no bad thing. Transparent yet safe, secure yet accessible - blockchains might just be what the Tim Berners-Lees of the world are looking for.

How SPARKL works

SPARKL is powerful technology for managing distributed systems. It's particularly applicable for orchestrating microservices, as well as making sense of data from the Internet of Things (IoT).

SPARKL is based on the concept of distributed intelligence, where multiple SPARKL instances work together to achieve a collective goal. It's also suited to regular orchestration of system components in the enterprise.

Common to all of these use case scenarios is **logging**. SPARKL orchestration produces clean and uniform event logs (or Audit Trails), which can be fed to analytics and mining tools for business reporting - making it easy for compliance teams to rapidly deploy business processes and smart contracts with complete transparency.



Example technology integration with SPARKL for both Process Execution and Analytics with respect to this execution, including over data provenance

SPARKL can be configured to record event logs in any database. The choice of analytics and mining tools is similarly flexible, and is determined based on the reporting needs of the business.

SPARKL comes with certain out-of-the box integrations to this end, as shown above. For example:

- HAProxy for high availability and initial load balancing
- Marathon Mesophere for docker cluster-based scheduling
- Docker for microservices container execution
- Logstash for collection of infrastructure logs from disparate environments
- Slamdata and Kibana for visualisation, analytics and business reporting

Blockchain-Powered SPARKL

SPARKL provides a simple, declarative modelling language, called Clear Box® which couples with the SPARKL Sequencing Engine to detect **anomalous** trends in log data, called **breakouts**.

This can readily demonstrate regulatory compliance and could be particularly useful for an Internet of Things (IoT) setting, such as drugs manufacturing. Possible breakouts can be confirmed as such by an administrator, so that the algorithm learns without requiring pre-training.

This is just one example where SPARKL helps to make sense of data that it logs, protecting them so that if an anomaly occurs, there is tamper-proof evidence of the fact.

At its heart, a blockchain is a tamper-proof, append-only log — so it's useful potentially anywhere that such a logging capability would be needed. There is plenty of value in being assured that event logs haven't been tampered with.

A blockchain is generally a chain of digitally-linked blocks of (e.g. currency) transactions. With SPARKL, we group **event digests** into blocks. So, a SPARKL blockchain is a chain of linked blocks of event digests, or hashes.

Blocks are linked in the sense that a hash or digest of the previous block is included in the next one in the chain. This means that if some nefarious party wanted to rewrite history by starting at block **X** in the chain, then every block subsequent to **X** would also have to be rewritten, a major undertaking in itself.

Lots of time, expertise and compute power would be required for a party to conceal their changes.

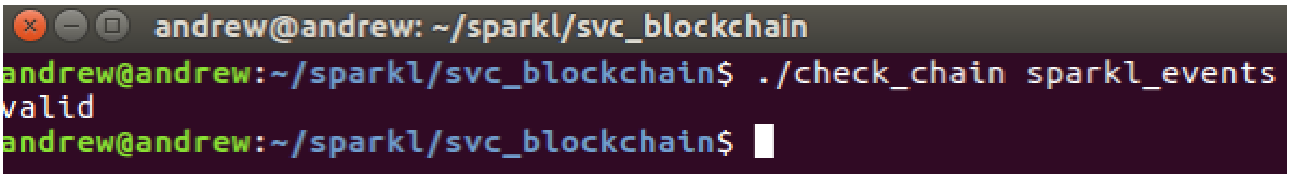
In the case of a traffic accident, event logs could be sourced from coincident pieces of infrastructure and vehicles. These logs could help city authorities to determine what happened, and would be protected from tampering by SPARKL.

With SPARKL, we push blocks of event hashes onto a blockchain, and keep this separate from SPARKL event databases. There isn't any need to actually record the events themselves on the blockchain.

A party cannot simply perform casual rewrites of event logs without the changes being exposed through reconciliation with the blockchain. Even with access to both the events and the blockchain, it requires significant effort to coerce undetectable changes to event logs. In this sense, SPARKL event logs are highly tamper-proof.

SPARKL makes available tools which an administrator or auditor can run on an event database to reconcile its contents with information maintained on a live SPARKL blockchain.

A common integration of SPARKL, as shown in the figure below, is with MongoDB. This enables analytics via SlamData, for instance. SPARKL provides a command-line tool which draws event data from a MongoDB database and validates it against a SPARKL blockchain. The tool will give an answer of '`valid`' or '`invalid`' with respect to whether event logs are valid. If '`invalid`', the tool will show where:



```
andrew@andrew:~/sparkl/svc_blockchain$ ./check_chain sparkl_events
valid
andrew@andrew:~/sparkl/svc_blockchain$ 
```

The code for the tool is notably simple and open to inspection, meaning that anyone can verify its function, and the use of blockchains makes it that much harder to tamper with the logs.

We have integrated with typical blockchain solutions, such as Hyperledger and BigchainDB. In the example of the traffic accident, there ***are*** advantages to using a public blockchain — with these, you can see their histories, making it nearly impossible to manipulate the facts. But private blockchains, like SPARKL, work sufficiently for many use cases.

Even if the owners of the public infrastructure or vehicles had the time, expertise and compute power to meddle with individual blockchains after the incident, the inconsistencies would be picked up when compared with the blockchains maintained by other involved parties - even if multi-party collusion is pretty unlikely.

Let’s talk

Go to sparkl.com to talk to us live or shoot us an e-mail at talk@sparkl.com.

@sparkl

See SPARKL tutorials and demos at
sparkl.com/docs/web