ORBS

Blockchain Virtualization: A Necessity for Real-World DApps

Oded Noam, Chief Architect, Orbs

Executive Summary

Analyzing the requirements dApps have from their blockchain infrastructure, we see similarities between their needs and and those of web applications in the early stages of web based consumer services. The infrastructure options for developers, then and today, can mostly be classified as either shared or dedicated infrastructure. The core technology that can resolve most barriers to mass market adoption, in both cases, is virtualization. In this paper we explore how virtualization solved significant barriers in web application backends, analyze the barriers experienced with current-generation blockchain technology, and explain how virtualization technology offers the potential to overcome these barriers. We predict some of the additional benefits such technology will bring to users, and detail how the use of virtualization at the core of the Orbs network enables it to be a superior solution for dApp developers.

Overview

As Internet applications made their way into mass-market adoption in the late 1990s, data centers providing back-end processing quickly became the behemoths of the industry. Initially, application operators had to choose between dedicated server hosting and shared hosting. The former allowed operators absolute isolation from other apps, and control of all factors including hardware, operating system and configuration, etc. The latter did not offer this flexibility - the app ran alongside others' in the same computer, and is subject to interference and even data theft from other apps running alongside. Naturally, shared hosting offered much better utilization of the servers and accordingly was and remains much cheaper to operate.

As virtualization technologies made their way to data centers, applications were able to select a third alternative: virtual private hosting. At almost the cost of shared hosting, applications can now have a completely isolated environment, control over the operating system, the configuration, and even some of the hardware resources allocated to them.

While this shift was triggered by cost considerations, what emerged from it opened the door to a cambrian explosion of innovation around another aspect of virtualized services: flexibility and elasticity. With close to zero set-up costs, application developers can (and do) make extensive use of elastic resource allocation not only to scale their systems, but also to fragment their systems for testing, systems, and mutations that perform multivariate testing of just about any variable in their operation, speeding up and lowering the cost of business innovation. It turned out that server virtualization had a profound effect on the evolution of application back-ends.

Blockchain technologies today are in the process of making a similar transition. Current generation platforms are either dedicated to a single application (like Bitcoin, Stellar, and numerous DApps that derived from relevant forks) or shared between all (like Ethereum or EOS), with pretty much the same costs and benefits that dedicated and shared hosting have. Newer platforms are mostly structured to provide each dApp with an isolated environment, or a virtual chain (sometimes also called *channels*, *parachains* or *workchains*). In this paper we will discuss the benefits of virtualization, and claim that it is an inevitable step forward in the evolution of blockchain technology and a crucial basis for modern DApps.

Impracticality of Dedicated and Shared Infrastructure Architectures

Practical implications of managing a private infrastructure

The barrier for a dApp developer wishing to set up a dedicated infrastructure is in fact much higher than setting up a centralized system on dedicated servers. Beyond forking a codebase of a blockchain protocol, the dApp developers would have to set up a decentralized network of independent validators, to operate the platform.

To operate a decentralized network of independent validators, each of these validators needs to be trustworthy, and technically capable of securing the network: properly set up secure servers to perform the block validation, review and approve the codebase for the protocol and any changes submitted to it, and participate in the discussion of protocol changes — in particular, audit the security implications of such. Such capabilities are rare and expensive, making this process almost impossible for the average dApp.

Sustainability of the validator network is an extension of this challenge. Sustaining a validator network is particularly risky when the network size is not sufficient (or marginally sufficient) for the platform to operate -- commonly referred to as the “critical mass” problem. At these small sizes, network validators gain little value from their participation, making it harder to grow the network beyond this threshold. To create an incentive for joining, many networks distribute parts of their core assets to first joiners, luring early adopters expecting high future gains in case the network grows successfully. Such tactics are inefficient in cases where the network is contracting in size, putting apps that experience a decline in usage at risk of fast abandonment of validators.

Due to the significant costs of bootstrapping a functioning validator network, and the persistent risks that sustaining it projects on the dApp's infrastructure, a single dApp may find it too hard to set up a dedicated network. This is especially true when the function of the blockchain platform is critical for the operation of the dApp. It is reasonable to assume that dApps that took this path did it for lack of reasonable alternatives, or due to underestimating the associated costs and risks.

Performance Predictability in Shared Infrastructure

While the use of shared infrastructure such as Ethereum or EOS relieves the dApp developer from the challenge of setting up a network of validators, it does put forward a series of barriers to practical use, because of challenges with performance, governance and security.

One aspect is predictability of platform performance. This type of predictability is crucial for application engineers to plan the system usage in such way that it is able to provide continuous service. The performance of non-isolated shared infrastructure, such as Ethereum, is inherently unpredictable due to the conflict between the tenants using shared resources: any congestion in one dApp inevitably spills over to all other dApps using the platform. A famous example of such failure was experienced by Ethereum dApps in December of 2017, with the emergence of "CryptoKitties", a crypto-assets based social game which clogged the Ethereum network causing transactions delays ranging from several hours to multiple days.

Beyond the problems associated with unpredictability, failures such as the "CryptoKitties" congestion expose a flaw in the application of market mechanics to regulate resource allocation in shared platforms. In shared platforms, as the supply of these resources falls short, some or all of the dApps using the infrastructure will have to suffer degradation of the quality of service. To manage short-supplied resources, Ethereum (and other platforms) apply market pricing to distribute the supply of resources: every transaction sender bids on gas price (multiplier to the transaction fee) for including her transaction in a block, and the miners maximize their revenues by including highest-paying transactions in their block up to its capacity limit. This ensures that block space will be allocated to the transactions worth most to their senders, ensuring the overall utilization of the system yields the highest total utility to all its users ("pareto efficiency"). Alas, the individual dApp may find itself in a hard spot: the usage fees may surge above their value to the dApp users, creating a dilemma between operating the dApp at loss and a disruption to the service.

Similar risks exist in markets of other means of production, such as energy or freight, and manufacturers can sometimes mitigate them using forward pricing markets for these resources. Blockchain fees markets today fail to provide a sufficient solution, due to price volatility being especially high, and unavailability of forward pricing markets (with the exception of EOS, in which token ownership can ensure throughput quotas, making the EOS token a forward market for block capacity in addition to its other uses).

Cloud platforms succeed in ensuring predictably-low costs by providing excess resources, to an extent that a realistic increase in demand for one app can occur without creating competition on the same resources with other apps. Without competition on a scarce resource, infrastructure prices remain proportional to the underlying operation costs. To

enjoy similar cost structures, blockchain platforms don't have to grow to the stage they're enjoying resource abundance, if they are designed to work on top of existing cloud platforms and make use of their elasticity of resource allocation. Working on top of high-capacity networks allows containerization into virtual chains, providing the dApps with the benefits of predictable quality of service at predictable cost.

Governance Problems Inherent to Shared Infrastructure

Usage of a shared infrastructure requires the community of users to agree on any changes to the underlying protocol. For the purpose of this analysis we will make the distinction between changes that are fixes and improvements to the protocol itself ("fundamental decisions"), or fixes to the contracts and data used by specific dApps or users ("particular decisions"). Note that some modifications can be considered both - for example, EIP-999[1] was designed to release funds lost by ParityMultisig users due to a smart contract bug, but is also as an improvement to the protocol that will eliminate similar losses for all users of Ethereum. It should be pointed out that governance institutions of most platforms do not make this distinction.

While there are many forms of governance practiced in blockchain platforms, it is widely accepted - for obvious reasons - that fundamental decisions should be considered and applied with great caution, in a particularly consensus-seeking and conservative approach, especially on a network that already hosts live dApps. When such an approach is applied to particular decisions, it surfaces a conflict between the dApp's stakeholders who see the merit of the change, and other users of the platform whose attitude towards the proposition is expected to be neutral or negative.

The history of protocol changes proposed in Ethereum that were meant to thwart larceny point out stark examples of this conflict. All but one were rejected: the only one that was famously ratified is "DAO Fork" (later filed as EIP-779[2]) of July 2016, which cancelled ETH transfers made by a hacker exploiting a reentrancy bug in TheDAO smart contract. This decision overtly contradicts Ethereum's proclaimed central principle, that a smart contract's execution is the sole interpretation of its intent ("code is law"). It has clear losers, actual addresses whose Ether is taken away from. Yet it was ratified by an astounding 89% majority, becoming the only such proposition to ever pass in Ethereum. One contrasting example is EIP-999, which was supposed to release Ether locked in inaccessible smart contracts following a famous accidental deletion of a code library used by the popular ParityWallet contract. This proposition fixes what can be considered a bug in the Ethereum protocol, it has no clear losers (it releases funds that are otherwise inaccessible) yet it was rejected with 39% for and 55% against.

While the specifics of the EIP-999 debate may have been pivotal to this outcome, the fact that EIP-779 is the only one to have ever been ratified indicates that interests rather than principles plays the major role in such decisions. And in fact, TheDAO hack in mid-2016 affected all of Ethereum's users because it publicly raised serious doubts about the platform's function (ETH exchange rates dropped nearly 40% following the hack). From the

[1] https://github.com/ethereum/EIPs/blob/master/EIPS/eip-999.md
[2] https://github.com/ethereum/EIPs/blob/master/EIPS/eip-779.md

perspective of the average Ethereum stakeholder, EIP-999 bears some risk of having unintended consequences and benefits only a few, and rejection of EIP-779 was likely to result in a major blow to the public trust in the entire Ethereum ecosystem from which everyone will be harmed.

The attitude of the governance institutions on particular decisions may vary depending on the level of isolation dApps get in a platform: in platforms that provide low levels of isolation, other users of the system will perceive any such change as an unnecessary risk that should be avoided. Such conflict is avoided in platforms that provide isolation, which tend to be more positive (or indifferent) towards such changes. EOS, for example, uses the EOS Core Arbitration Forum (ECAF) as a semi-judicial body that can make changes to smart contracts, lock addresses and modify data. Though this arrangement is relatively new, it so far appears to have an active and progressive approach, in contrast with the conservative nature of the governance of earlier shared blockchain platforms. However, such institutes and their activities raises questions about the risks and implications of delegating such decisions to non-stakeholders in the dApp. Communities should be wary to place their fate in the hands of a committee that is, at best, indifferent of the consequences of its decisions.

Incongruity of the Shared Platform Security Model

The common security model of public blockchain platforms was designed for dedicated platforms that serve a single dApp. The security models for both proof-of-work and proof-of-stake are dependant on a proportion between the risk invested in mining blocks to the total value of the ledger: the fundamental idea is that miners risk monetary assets (pay energy costs in the case of proof-of-work, stake crypto-assets in the case of proof-of-stake) that will only pay back if the blocks they produce are recognized as valid by the other miners. The level of risk taken by miners is therefore determined by the expected reward, which is generally determined in proportion to the total value of the circulating crypto-asset (through the mechanism of predetermined inflation in supply).

When this mechanism is used in public smart-contracts blockchain platforms, the native infrastructure token value is determined independently of secondary assets that are managed on the ledger. Plainly, growth of a dApp's assets that is unproportional to that of the underlying platform puts the entire platform at risk. Moreover, an aggregate of assets that together grow beyond proportion to the underlying platform impose similar risk. The ordinary process of widely-used infrastructure becoming a commodity over time will inevitably disconnect the value of any general-purpose platform from that of growing DApps. Such disconnect has a destabilizing and potentially devastating effect on the security of shared platforms.

Applying Virtualization to Decentralized Platforms

As with centralized backend technologies, the introduction of virtualization to blockchain platforms has the potential to resolve many of the practical barriers to adoption, while simultaneously introducing significant improvements. The fundamental architecture of a virtual blockchain platform is that of a common *decentralized* network of validators, each participating in the validation of multiple separate ledgers. The protocol consists of two

separate layers: a layer managing the validator network (this is parallel to the role of a hypervisor in centralized virtualization), and an application layer with a separate instance per virtual chain.

New Possibilities in Virtualized Blockchains

In fully-virtualized platforms, separation in the application layer means that the consensus protocol, smart-contracts virtual machine, state storage and blockchain storage of each virtual chain are independent of each other.

Many of the typical problems that are inherent to dedicated and shared platforms can be avoided in this architecture[3]. In every virtual chain, since block rate and size can be assumed, and since the contents of the blocks is dedicated to a single dApp, the multiple of the block rate and size yields its guaranteed throughput. Flexible allocation of virtual chains ensures there is no competition over network capacity, reducing the risk of price increases due to surges in demand. Governance of the meta-layer protocol is shared between all users of the network and follows the conservative approach, but with a high level of alignment between the parties. Governance of each virtual chain is determined by its own stakeholders and is expected to choose more progressive approach, gradually reducing towards conservatism as the DApp matures. And, virtual chains can select their own native token, opening the door to safe use of proof-of-stake.

Recall, for example, the case of the ParityMultisig bug. It would be most beneficial to the community of ParityMultisig users to have had the authority to change the protocol as proposed in EIP-999, without affecting other contracts deployed on the Ethereum network.

Such architecture also enjoys a new level of flexibility that was not achievable in previous designs. Since it enables deployment of virtual chains without the costs and delays of setting up new decentralized validator networks, it can be used to enable dApps to experiment more often, mutate, fork their contents, apply multivariate testing and further techniques that can expedite product development. Flexibility with parameters of virtual chains, such as block rate, choices of cryptographic protocols and addressing schemes, consensus protocols, and on-chain governance schemes has the potential to expedite evolutionary processes in the development of core blockchain technologies.

Orbs' Virtual Chains Implementation

Orbs is designed from the ground-up as a virtual chains container platform. The network meta-layer is managed by the Orbs management virtual-chain, that operates as a regular virtual chain but has special permissions to modify the meta-layer parameters. Virtual chains can be deployed or destroyed using smart contracts calls in the management chain.

Deployment of a virtual chain means static allocation of the required resources for its execution, which means that once one is deployed it enjoys a guaranteed quality of service for the dApp using it. If resources are unavailable, the virtual chain will not deploy. To prevent

[3] For further analysis of how virtualization solves problems typical to shared and dedicated platforms, please refer to our working paper *Blockchain Architecture to Mimic Cloud Services*.

scarcity of virtual blockchains to be a pivot for price increases, the system is designed to scale out horizontally mostly on compute instances and bulk storage space, which are the most elastic resources on traditional cloud platforms, while avoiding increases inside bottlenecked silos such as compute instances and core network traffic. This ensures that node operators running on top of traditional cloud platforms can scale their capacity almost indefinitely at a *constant* marginal cost.

Every validator in the Orbs network is participating in the validation of all virtual chains, and her profits are proportional to the amount of validations her node can process. Since capacity can be horizontally increased indefinitely, and the additional fees result in additional revenue per virtual chain, validators will increase the overall system capacity with demand.

In the application layer, setup of virtual chains can vary on a number of important parameters:

- **Block size and frequency**, which together determine the guaranteed throughput of the virtual chain;
- **Consensus protocol**, which can be selected out of a pool of protocols supported by the platform. The different protocols vary on latency, security, fairness and other properties;
- **Cryptographic scheme**, where different schemes vary on their support for group signatures, security of the setup process, compatibility with cryptographic hardware, and compatibility with other protocols;
- **Addressing scheme**, where different schemes are compatible with different schemes of other platforms, allowing a virtual chain to support addresses derived from public-private key pairs that are used on other blockchain platforms; and
- **On-chain governance scheme**, allowing every dApp to choose or define its stakeholders and voting methods according to its needs. dApps can choose, for example, to use proof-of-stake or delegated proof-of-stake (with stake determined in tokens managed inside the virtual chain), proof-of-authority, consortiums, centralized control, quadratic voting and more.

We believe that beyond the immediate utility dApps can benefit from having such flexibility, it will benefit the entire blockchain community by expediting an evolutionary process in which contemporary techniques will improve and newer ones will be introduced.

---

info@orbs.com