dispersive

```
PUBLIC INTERFACE IGUIFACTORY
PUBLIC IBUTTON CREATEBUTTON
}

PUBLIC CLASS WINFACTORY
@OVERRIDE
PUBLIC IBUTTON CREATEBUTTON
RETURN NEW WINBUTTON
}
}

PUBLIC CLASS OSXFACTORY
@OVERRIDE
PUBLIC IBUTTON CREATEBUTTON
RETURN NEW BUTTON
}
}

PUBLIC CLASS WINBUTTON
@OVERRIDE
PUBLIC VOID PAINT() {
SYSTEM.OUT.PRINTLN(
}
}

PUBLIC CLASS OSXBUTTON
@OVERRIDE
PUBLIC VOID PAINT() {
SYSTEM.OUT.PRINTLN(
}
}

PUBLIC CLASS MAIN {

PUBLIC STATIC VOID MAIN
IGUIFACTORY FACTORY =

FINAL STRING APPEARANCE

IF (APPEARANCE.EQUALS
FACTORY = NEW OSXFACTORY
} ELSE IF(APPEARANCE
FACTORY = NEW WINFACTORY
} ELSE {
THROW NEW EXCEPTION
}
FINAL IBUTTON BUTTON

BUTTON.PAINT();
}

/**
* THIS IS JUST FOR THE SAKE
* WITH ABSTRACT FACTORY
* @RETURN
*/
PUBLIC STATIC STRING
FINAL STRING[] APPEARANCE
```

AUTHORS

Rick Conklin
Dispersive Networks
Chief Technology Officer

Ben Murray
Pulse Lab
Founder and CEO

In partnership with
the **Silicon Valley**
Blockchain Society

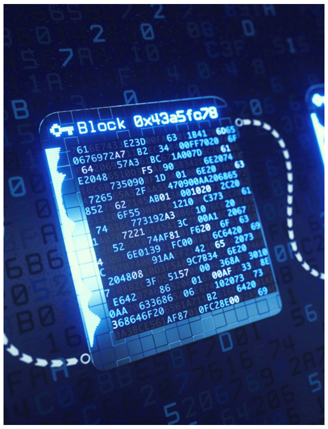
SECURING ENTERPRISE BLOCKCHAIN WITH SDN

ABSTRACT

While the decentralized data management and integrity capabilities that blockchain brings to enterprise applications are exciting, distributed ledger implementations are more secure when they run over highly secure, resilient, and fast virtual private networks. A layered approach to blockchain design will accelerate the adoption of large scale, mission-critical solutions particularly in industries where sensitive data is exchanged: healthcare, financial services, military, and government applications, energy grid, and others. In this white paper, we'll share insights on how programmable networking can be fused with blockchain data integrity, access and document management, and compliance requirements solutions to not only secure computing and collaboration environments but to validate them using distributed ledger approaches.

EXECUTIVE SUMMARY

Securing data at rest or in motion is accounted for on any blockchain with immutability whether moving across public or permissioned blockchains. Fusing together the software on all layers of the technology stack creates advantages for service providers rolling out the next generation of secure, real-time data exchanges. The transmission network can no longer be an afterthought. Service providers can offer unprecedented service-level agreements for performance and protection by bundling virtualized networking which runs over the public Internet but in highly secured sessions with blockchain-based solutions.



Enterprise blockchain is still in its infancy, but it will inevitably change the IT landscape forever. The benefits of Network Function Virtualization (NFV) and Software-Defined Networking (SDN) can now be brought together with the benefits of the distributed ledger, so more complex, high value, mission-critical applications can be rolled out without the risk of "unexpected consequences" seen in situations like the early DAO hack.

IP networking and the very architecture of the Internet make sense for blockchain when we delaminate it. Each Internet layer is more abstract than the lower layer until we get to the physical transport layer. This is the fundamental reason the Internet is robust and the most resilient network in the world. Why? Because each layer can be upgraded, patched, or even replaced without affecting other layers.

In this white paper, we'll explore how software-defined networks designed to support mission-critical applications leveraging the public Internet over which virtual networks are spun up and managed are "rocket fuel" for new blockchain-based applications. We'll articulate what is now possible at the session layer, which manages the highest-level connection states running immediately above the transport layer. We'll share an engineering look at innovative ways to blend session and application layer security and performance management in blockchain use cases.

We will demonstrate how SDNs can work together with Smart Contracts and provide the flexibility that addresses different needs depending on the nature of the community and data interactions, and requirements for transparency, on the one hand, opacity on the other. We'll touch upon audits and compliance and how this "fusion" can improve the efficiency of oversight and management.

We'll also explain how blockchain's layers (consensus, mining, propagation, semantic, and application) dovetail with network layers to drive feature functionality, policy, and above all—control.

Finally, we'll share examples of how real-time communications between machines (The Internet of Things) and people can be authenticated more elegantly when the network itself becomes part of the blockchain solution. This addresses massive gaps in terms of privacy and security by ensuring every endpoint—every application—every cloud—and every privileged administrator with credentials to make changes in "the system" can be controlled and verified—whitelisted and blacklisted—and compliant with increasingly strict regulations in our rapidly, digitally transforming world.

MORE SECURE DISTRIBUTED LEDGER ENTERPRISE SYSTEMS WITH SDN

Combining Virtual Networking and Blockchain for Iron Clad Solutions

The massive growth of data and data sharing is putting pressure on traditional networks. Modern, secure networks must be much more dynamic, and much easier to set up, while at the same time harder to attack.

Software-Defined Networking enables on-demand provisioning of network elements much more effectively than traditional, equipment-heavy and costly networks, and this is driving enterprises (and the service providers who support them with bandwidth and applications) to move to SDN.

Drivers of network pressure including increasingly higher end-user expectations, on-demand services available on mobile devices, high-definition video for rich collaboration applications especially for remote workers and as part of partner and field service applications, unpredictable and large traffic flows including those associated with "incidents," and the economics of virtualization and desire to move to Commercial off the Shelf (COTS) or generic, non-proprietary servers.

Additionally, the networking solution selected for the blockchain ecosystem must be easy-to-use and easy-to-integrate into existing networking platforms, networking technologies, and security profiles. The connectivity for applications and things should ensure authentication-before-access, micro-segmentation of services, and easy-integration with network address translation tables and firewalls. The networking solution must "just work," and it must do so securely regardless of the underlying network topology which may include, but is not limited to, 5G, 4G, LTE, Wireless, Wireline, IPv4, IPv6, LoRa, SoDeRa, BLE, and Cloud Resources.

> With so many opportunities for improvement, enterprises and organizations, including government agencies and educational/research institutions are opting into SDN but are concerned about how to secure and validate transactions and events moving across SDNs.

5 billion
records breached in 2018

81%
of breaches due to stolen passwords

43%
of the successful breaches were linked to internal actors

$3.86 M
Average cost of a data breach

Sources: https://breachlevelindex.com/ IBM Cost of Data Breaches, CA Insider Threat Report, McAfee Grand Theft Report, Verizon DBIR Report

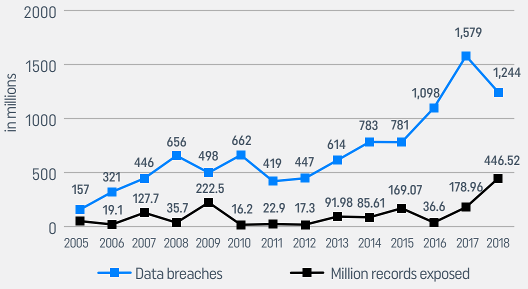
Security breaches cost
$600 billion
a year globally

Insiders contributed to
46%
of cybersecurity incidents in 2017

30%
of security professionals expect a major and successful attack within 90 days

Sources: McAfee and the Center for Strategic and International Studies, 2018.
Kapersky Lab. "The Human Factor in IT Security." 2018
The Economist Intelligence Unit, "The Cyber-Chasm. How the Disconnect Between the C-Suite and Security Endangers the Enterprise." 2016

Annual number of data breaches and exposed records in the US from 2005 to 2018



Source: Indentity Theft Resource Center ©Statista 2019
Additional Information: US; Indentity Theft Resource Center; 2005 to 2018

No Industry is Immune

WHOLE FOODS MARKET
IHG InterContinental Hotels Group
verizon
UNITED STATES POSTAL SERVICE
facebook
LabCorp
Panera BREAD
Marriott
BLACKROCK
YAHOO!
Quest Diagnostics
Microsoft
AdventHealth
CHIPOTLE MEXICAN GRILL
Deloitte.
EQUIFAX
FEMA
CITRIX
WhatsApp
DUNKIN' DONUTS
BRITISH AIRWAYS
DOW JONES
UNDER ARMOUR
GMail

REDUCING THE PROBABILITY OF INTERCEPT

Mitigating the Risk of Adversaries Identifying and Recording Flows of Interest

A common vulnerability found in today's blockchain-based systems is the ease with which attackers can exploit flows of interest. Typically, they identify these by source or destination IP address, or by source or destination port, or by inspecting information that is sent in the clear.

For example TLS 1.2 and DNS can leak information that is useful in flow identification because certain information (TLS headers, certificates, DNS requests, and more) are sent clear text.

In this scenario, an adversary can store the entire flow for later analysis. This is problematic given that a TLS protected flow will exchange key negotiation (e.g., Diffie-Hellman or Elliptical Curve Diffie-Hellman) over the same flow as the encrypted data of value.

The Chain

1. Adversary identifies flows of interest
2. Adversary captures entire flows
3. Systems A and B negotiate a key using DH or ECDH
4. Systems A and B encrypt data using symmetrical encryption (e.g., AES-GCM)

Items 1-4 happen on the same flow/IP quad.

An adversary can capture the entire flow and process it later. If the Adversary is able to melt the encryption in the key negotiation, the adversary can break the entire chain.

Blockchain Based Applications May Be Especially Vulnerable to This Problem

Capturing that data and melting the encryption is expensive; however, advances in cost-to-compute, advances in mathematics (e.g., to solve the discrete logarithm problem), and/or advances in quantum computing can place captured data at risk.

At a minimum, blockchain-based applications should use a virtual networking technology that ensures low probability of intercept.

Blockchain is Not Inherently Secure

In total, hackers have stolen nearly $2 billion worth of cryptocurrency since the beginning of 2017, mostly from exchanges, according to the MIT Technology Review.

Sophisticated cybercrime organizations are attacking blockchain systems; analytics firm Chainalysis reported that just two groups, both apparently still active, may have stolen a combined $1 billion from exchanges thus far.

Binance, a popular cryptocurrency exchange was hacked in 2019, a loss estimated to be worth $40 million. Hackers were able to obtain user API keys, 2FA codes, and other information in a single transaction, withdrawing 7,000 Bitcoins.

NETWORK LAYERS AND NEW SESSION MANAGEMENT TECHNOLOGIES

By integrating security into the network itself, advanced SDNs address the challenges of security, scalability, and auditability.

Not all SDN technologies are alike. And not all SDN business applications are "mission-critical." For industries where real-time communications and compliance are essential (financial services, healthcare, energy grid, military and government, public safety, and others) ensuring the quality and privacy of every session is table stakes.

The shift towards SDNs opens up new attack vectors for hackers when the network can be addressed by APIs, and not just connected servers as is the case in the current and old networking paradigm.

SDNs also support multiple participants, multiple clouds, multiple applications, entire supply chains, data exchanges and "uber collaboration" whether automated (machine to machine) or automated including humans (administrators, traders, and others).

The volume of entities that may connect to SD-based networks raises the scalability question: how can the ecosystem ensure that one bad apple can spoil the whole bunch when a rogue element among thousands may be compromised and pivoted to take down the entire network?

We can start with a new generation of SDN, where sessions are treated in such a way to prevent "man in the middle" attacks on data in motion by authenticating and authorizing each endpoint before it gains access to the network.

We can then layer in solutions that control administrative access, tracking, storing, and validating every event (machine or human) and triggering alerts when anomalies occur. Authentication-Before-Access, Zero Trust, Micro-segmentation, and machine time monitoring (AI, ML, DL) are the answer, and with the right architectural approach can be harmonized with layers of blockchain capabilities.

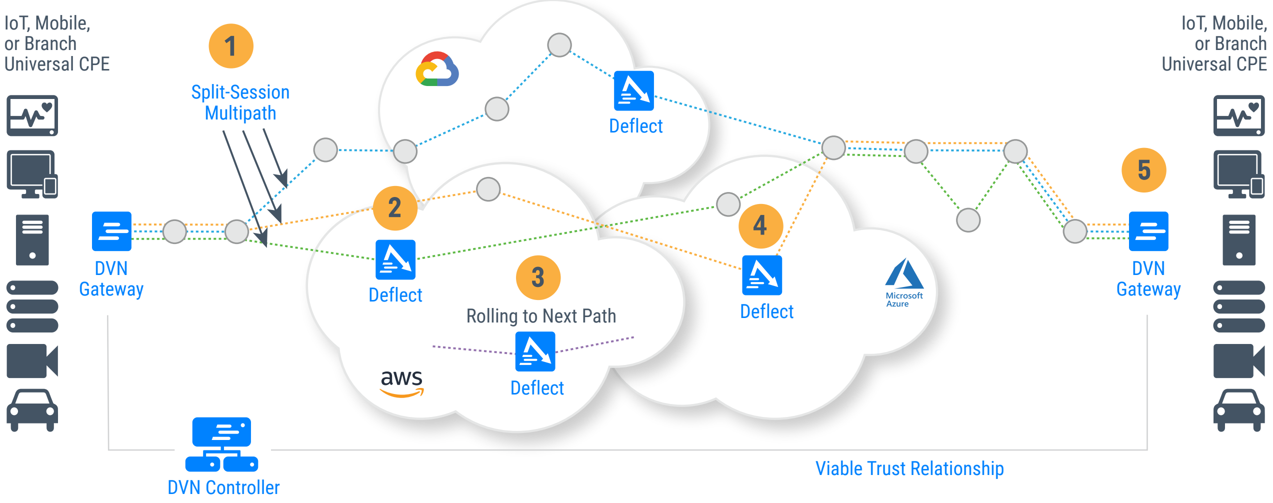
Authentication and Authorization before Access

An adversary can only see that an endpoint is sending and receiving information and flows are difficult to detect and assemble due to traffic splitting. This is a combination of the DVN principles of managed attribution (MA) and low-probability-of-intercept (LPOI). Authentication and Authorization before Access (AAbA) mitigates attack vectors applied to a server including infiltration, FIN/ACK, TCP Shill, DoS, DDoS, etc. In other words, MA/LPOI handles passive eavesdropper attacks, while AAbA mitigates network mapping, server discovery and the active attacks that follow that discovery phase.

ANATOMY OF THE DISPERSIVE™ VIRTUAL NETWORK (DVN)

A DVN deployment is composed of three fundamental components: end point clients/gateways, strategically placed deflects, and controllers.

The Multi-Path/Multi-Cloud Approach



Step 1

Data streams are split at the authenticated source and re-addressed with a DVN header to force traffic to follow different network paths based on instructions from the DVN Controller across one or more physical circuits.

Step 2

The underlying IP networks deliver these packets to DVN software nodes known as data Deflects. Placement of these deflects influences the actual physical paths traversed.

Step 3

New paths can be established/rolled during the transmission enhancing performance by avoiding link failures and bypassing congested pathways.

Step 4

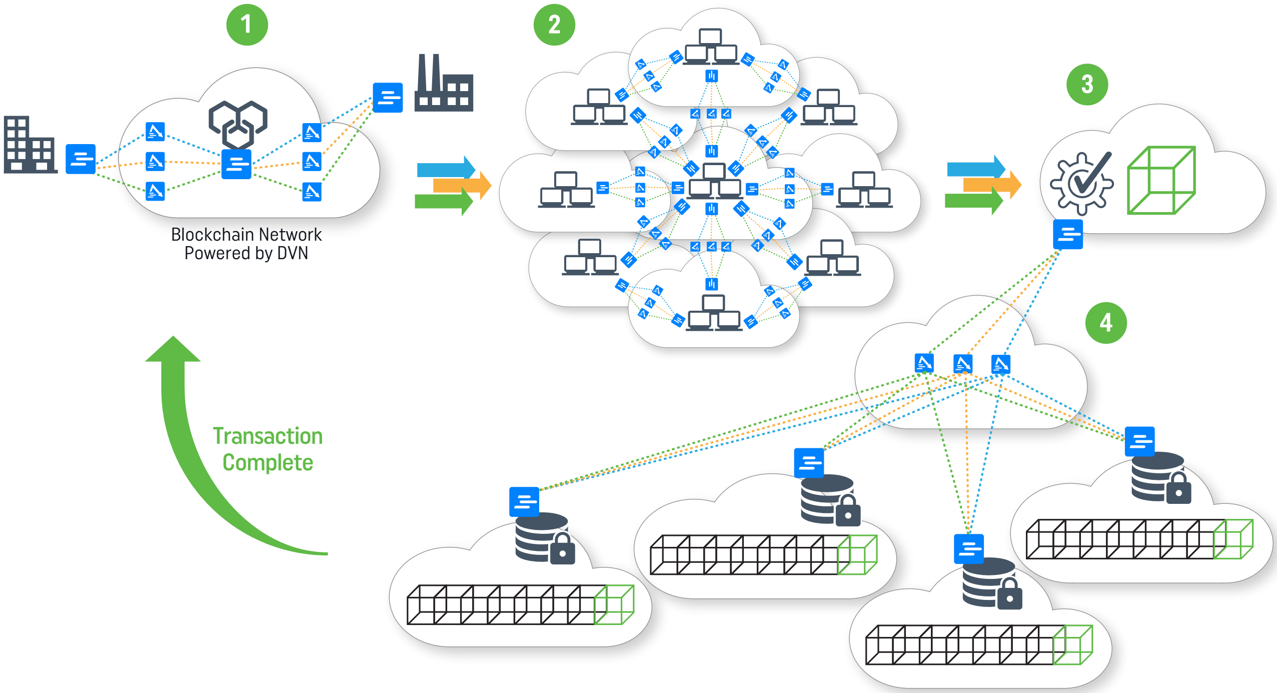
The data Deflects receive the packets and re-address them for the final destination.

Step 5

The authenticated destination reassembles the split packet streams and strips out the DVN header information before passing the original packet to the receiving application. Missing packets are re-requested to ensure guaranteed packet delivery.

BRINGING IT ALL TOGETHER

The DVN enabled blockchain network is a virtual overlay that operates agnostically over multiple clouds, networks and access transport providing maximum flexibility, security and resiliency to the blockchain.



Step 1

Settlement event between two enterprises. Edge to cloud is addressed using Dispersive™ Virtual Network (DVN) edge gateways between parties and the blockchain platform.

Step 2

The requested transaction is broadcast to a P2P virtual network of nodes, all of which have DVN edge software and can communicate with each other, while residing on different clouds/networks and without the use of VPN. All endpoints are authenticated and authorized before they gain access to the network.

Step 3

The nodes validate the trasaction. Upon verification, the transaction is combined with other transactions to create a block of data.

Step 4

The block of data is added to the distributed ledger. The distribution of the block to the ledger is performed within the virtual network, fully private to the trusted entities that are part of the blockchain network.

Symbiosis and Synergies

Blockchain enables verification of transactions via distributed network authorization and then adds that data to an immutable ledger. The decentralization eliminates control by any one node, removing the risk of single-point failures. Because each transaction is transparent to all participants on public or permissioned blockchains, data integrity can be optimized.

Software Defined Networks (SDNs) support real-time application performance, an ideal fit for a blockchain architecture layer. Blockchain-enabled enables verifiable information-based transactions between network devices. The job of network admins can be more automated, and with additional enhancements, including Artificial Intelligence (AI) running continual analyses, unusual activity can trigger notifications to optimize the blockchain-enabled SDN.

At the same time, SDNs with the appropriate architecture can dramatically improve performance (speed), availability and overall security.

BY FUSING BLOCKCHAIN APPLICATIONS WITH INHERENTLY SECURE SDN TECHNOLOGIES, LAYERS OF PROTECTION CAN BE ORCHESTRATED ELEGANTLY

Blockchain IT Applications:

- Ensure every access point is automatically monitored with all activity recorded
- Control (whitelist or blacklist) authorized, trusted entities and administrators
- Ensure any rogue devices are detected and rejected in real-time, sending notifications to authorized administrators
- Create forensic logs
- Track every entity creation, deletion, valid or hack attempts, and store that in the blockchain, free from any possibility of tampering
- Leverage blockchain as a "gateway" into the SDN
- Allow for security audits
- Deliver additional layers of security, scalability, and auditability to SDNs

Annual revenue for enterprise applications of blockchain will increase from approximately $2.5 billion worldwide in 2016 to $19.9 billion by 2025, representing a compound annual growth rate (CAGR) of 26.2%

Source: Tractica

Programmable Networks:

- Ensure that every application, user, or device is authenticated and authorized before any network access is granted.
- Micro-Segment services so the application, user, or device may only access the specific applications, servers, or services that are authorized.
- Revoke access at any time -or- provide access during specific windows.
- Log performance monitoring data that may be processed, at machine time, by AI/ML/DL agents to detect anomalies, intrusion, or attacks.
- Merge IPv4 and IPv6 networks and deconflict network spaces.
- Ensure Confidentiality, Integrity, Access, Availability, Authentication, and Authorization for data-in-motion.
- Leverage blockchain capabilities for Identity, Authentication, Non-Repudiation, and Attestation.
- Provide RESTful API access for all provisioning and monitoring functions to ensure machine time velocity.
- Separate the Configuration Plane, the Control Plane, and the Data Plane to provide Zero- Trust and Zero-Touch-Provisioning while simultaneously mitigating many known attack vectors.
- Ensure High Availability through network redundancy, server redundancy, load balancing, and geographically-based connection and delivery.

SCALING SECURE NETWORKING FOR DECENTRALIZED BLOCKCHAIN-BASED IT SYSTEM ROLL-OUTS

Any SDN solution for Blockchain-Based Applications must be platform-agnostic and it must scale.

Platform-agnostic means that the SDN application must run on any platform including but not limited to Windows, Mac, Linux, iOS, Android, and/or IoT.

Scale means that it must scale to hundreds-of-thousands of endpoints and beyond. Some Blockchain-Based Application may require scalability to millions of endpoints, and the SDN solution must be capable of meeting that challenge.

An often under-looked aspect of security is Availability. Availability, in a secure environment, means High-Availability. That means a highly redundant Configuration Plane, a highly redundant Control Plane, and a highly redundant Data Plane where every server, orchestrator, and infrastructure node supports an M:N redundancy model for a High Availability architecture.

A Decentralized Blockchain Based system requires the SDN to support easy-to-deploy zero-touch models that can communicate regardless of firewalls, network-address-translation, or IT security perimeters. The SDN must support network plug-and-play where it "just works" without the need for IT support or the digital skills of a network engineer.

THE FUSION OF A BLOCKCHAIN & IP NETWORK STACK

The Ethereum Example

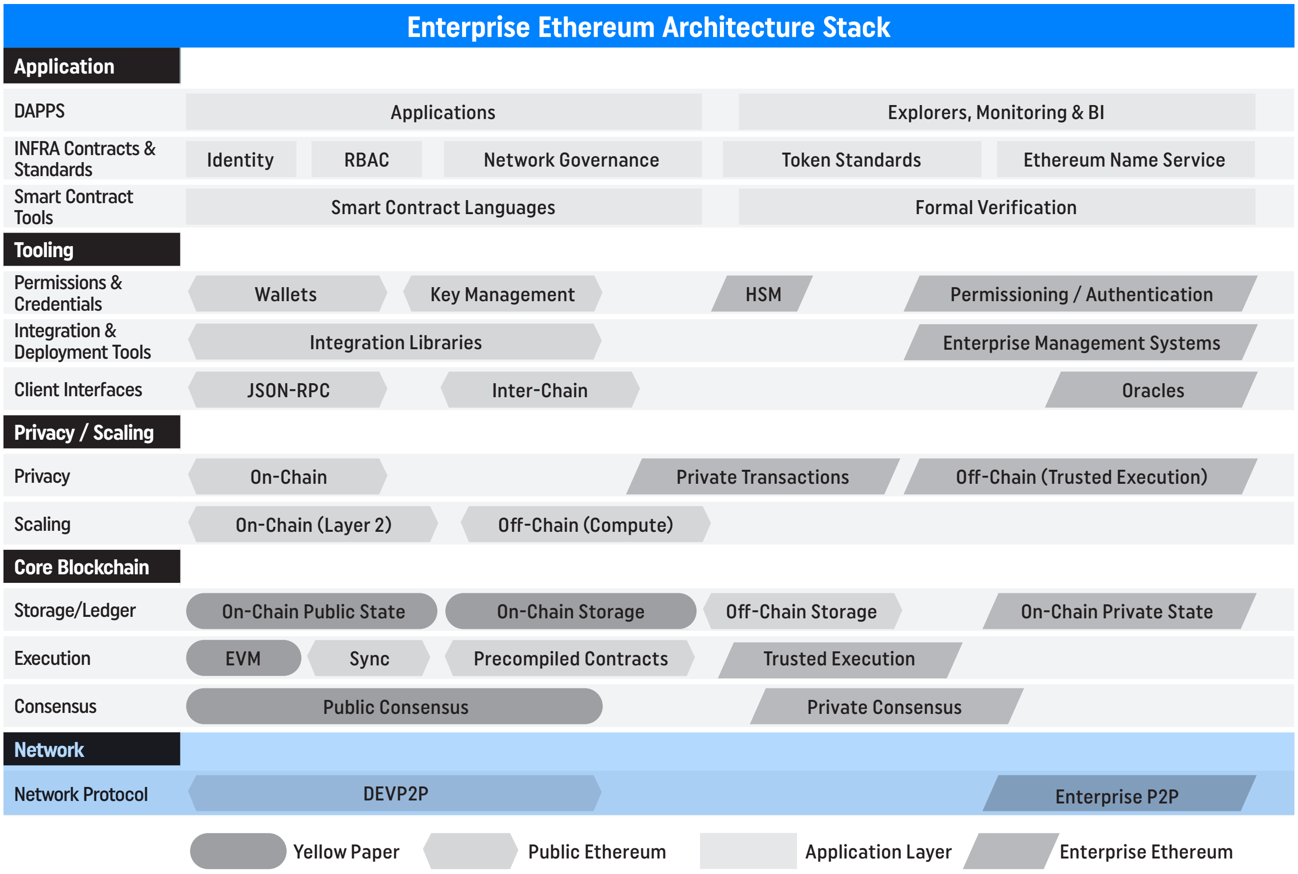
The Open Systems Interconnection (OSI) networking reference model continues to drive the development of secure private IP network architectures and solutions, and with the right technologies serves as the foundation for secure, scalable and resilient distributed blockchain systems.

OSI Model

Layer			Protocol Data Unit (PDU)	Function
Host Layers	7	Application	Data	High-level APIs, including resource sharing, remote file access
	6	Presentation		Translation of data between a networking service and an application; including character encoding, data compression and encryption/decryption
	5	Session		Managing communication sessions, i.e., continuous exchange of information in the form of multiple back-and-forth transmissions between two nodes
	4	**Transport**	**Segment, Datagram**	**Reliable transmission of data segments between points on a network, including segmentation, acknowledgment and multiplexing**
Media Layers	3	Network	Packet	Structuring and managing a multi-node network, including addressing, routing and traffic control
	2	Data Link	Frame	Reliable transmission of data frames between two nodes connected by a physical layer
	1	Physical	Symbol	Transmission and reception of raw bit streams over a physical medium

The New Fusion

The Ethereum/devp2p is the shim layer between the OSI layers 7-5 and the transport layer. The Ethereum/devp2p is not layer 4, itself. A virtual network technology like the Dispersive™ Virtual Network securely transports Ethereum/devp2p, and it plugs in at layer 4.



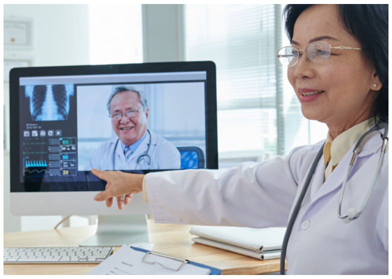
Enterprise Ethereum Architecture Stack

Application	
DAPPS	Applications Explorers, Monitoring & BI
INFRA Contracts & Standards	Identity RBAC Network Governance Token Standards Ethereum Name Service
Smart Contract Tools	Smart Contract Languages Formal Verification
Tooling	
Permissions & Credentials	Wallets Key Management HSM Permissioning / Authentication
Integration & Deployment Tools	Integration Libraries Enterprise Management Systems
Client Interfaces	JSON-RPC Inter-Chain Oracles
Privacy / Scaling	
Privacy	On-Chain Private Transactions Off-Chain (Trusted Execution)
Scaling	On-Chain (Layer 2) Off-Chain (Compute)
Core Blockchain	
Storage/Ledger	On-Chain Public State On-Chain Storage Off-Chain Storage On-Chain Private State
Execution	EVM Sync Precompiled Contracts Trusted Execution
Consensus	Public Consensus Private Consensus
Network	
Network Protocol	DEVP2P Enterprise P2P

All Yellow Paper, Public Ethereum, and Application Layer components may be extended for Enterprise Ethereum as required. ©2018 Enterprise Ethereum Alliance

INDUSTRY USE CASE EXAMPLES

Healthcare



The blockchain applications across the healthcare data spectrum are numerous. They include securing the immutability of medical records (which are often stored in silos), as well as maintaining the privacy of that data, as is compliant with HIPAA and patient health information protection laws. Blockchain solutions make it possible to share data securely, reducing the time it takes to access a patient's medical history and reduce errors associated with non-harmonized data.

Blockchain solutions can also create true data ownership, where the patient is in control of their own data and where usage of that data is fully transparent across the health system. Blockchain maintains an audit of transactions recorded through the Proof of Authority (PoA) mechanism, increasing the integrity of medical information through decentralized ledger approaches, and increases transparency between medical institutions by putting all data associated with a patient on a single chain.

Insurance

Insurance requires the coordination and cooperation of many different intermediaries where each step is part of a collaborative process, which can represent a potential for failure in the overall system. Without automation and governance, information can be lost, policies misinterpreted, and settlement times lengthened. Today, most agreements and claims are processed on paper contracts and require human intervention and lead to high error rates.

Blockchain technology is a cryptographically secured form of shared record-keeping, tracking, and auditing, and has applications in many areas of the insurance industry. For example, by moving insurance claims onto an immutable ledger, blockchain technology can help eliminate common sources of fraud in the insurance industry. Claims management, payments, and prior authorization can be integrated easily into the chain for more efficient payment processing. By securing reinsurance contracts on the blockchain through smart contracts, blockchain technology can simplify the flow of information and payments between insurers and reinsurers.

Financial Services

Distributed ledger technologies are being used across the many areas of financial services, including trading, consumer banking, commercial banking, lending, credit card services, and the rapidly changing world of payments.

Blockchain-based trading platforms aim to lower the cost of investing by reducing who takes a cut of each transaction. There are numerous middlemen between a stock buyer and a seller. A single trade might involve stockbrokers, depositories, banks, and clearing corporations.

Blockchain provides real-time compliance and improves transparency and audit, with greater oversight, which promotes responsible trading practices. Blockchain's shared electronic ledger helps them cut costs and increase efficiency. For example, Investment Banks can accelerate execution, post-trade processing, and settlement, which eliminates many middle- and back-office processes and reduces related errors. Blockchain-based money-transfer service payments can be made and settled in minutes via blockchain, rather than in days as with current systems.

Blockchain technology also enables customers to control and share personal data without the help of an intermediary through individual management of private keys (digital signature used to approve transactions). Several operating systems and browsers provide key stores to protect private keys, and private vendors offer wallets and similar alternatives that are resistant to cyberattacks.

Blockchain is also spurring innovation in the financial services industry with new applications being created which automate routine tasks, simplify regulatory audits, and otherwise drive efficiencies in the next generation of IT systems.

Retail

Blockchain enables smart contracts to be used within retail, an industry where success and profitability are increasingly related to logistical efficiency. The security features and the ability to record all steps in a transaction using smart contracts, for example, fit perfectly where ownership of products is transferred. Smart contracts are very transparent, meaning all parties can see everything that happens on a particular transaction, making it possible to track clear ownership rights across a large variety and quantity of products. These same smart contracts can alleviate the hassles associated with collection and enforcement under traditional transaction structures (instant collection and payment, automated refunds, automated insurance settlement, and payout, for example).

Blockchain will also allow retailers to accept cryptocurrencies along with digital records that will help streamline the refunds and return processes. Cryptocurrencies offer real advantages for both cross-border payments and micro-payments. Companies like Expedia, Overstock, and Newegg are already accepting bitcoin as a payment method. Most attention for immediate use of blockchain focuses on consumer payment applications, where customers complete transactions in cryptocurrencies. The size of payments and a large number of international transactions make cryptocurrency settlement an attractive proposition. Additionally, **the end-to-end data trail that blockchain provides, when applied to areas such as supply chain and inventory management, ease the accounting and finance burden.**

Supply Chain

Blockchain technology ensures integrity and traceability across the supply chain. The technology brings transparency and efficiency, which allows manufacturers, shippers, and customers to aggregate, monitoring, analyze data, look for trends, and perform AI analysis.

Blockchain uses track and trace processes to manage inventory along the path of the supply chain and can thwart against counterfeiter products since the entire chain is monitored and secure. Blockchain's transparency can also help reduce fraud and streamline the contract process between different suppliers and users.

Energy Grid

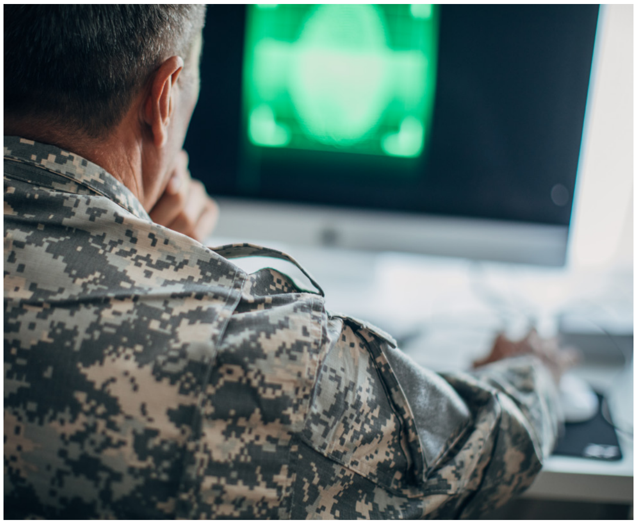
The U.S. energy sector, with its connected grids and dependence on computing and connected technologies, may be the most vulnerable point for a critical cyberattack. The energy industry was the most targeted sector by hackers in 2014, with 79 incidents recorded. Roughly 55% of those attacks were conducted by advanced persistent threats (APT), which is a way of saying that they were sophisticated hackers.

Blockchain technology has been implemented in the energy industry purely for its ability to be an immutable record. Blockchain is currently used to record, store, and track energy data, including market prices, marginal costs, energy law compliance, and fuel prices. Blockchain has established transactional digital platforms that are completely decentralized and can enable P2P energy trading, which allows for local energy marketplaces and Internet of Things (IoT) applications that can play a significant role in the smart grid.

Blockchain brings cost savings and efficiency improvement in the operation of energy systems and markets which can prove significant. Blockchain is also helping create "micro-grids," which are self-sustainable apart from the national grid.

Micro-grids currently exist as a layer on top of the grid. However, P2P blockchain energy companies imagine a future with larger, entirely distributed, interconnected peer to peer grids that allow participants to buy and sell renewable energy at even cheaper costs than before. **Blockchain-enabled transactional digital platforms could offer operational cost reductions, increased efficiency, fast and automated processes, transparency, and the possibility of reducing capital requirements for energy firms.**

Government & Military



NATO, along with the U.S. Defense Advanced Research Projects Agency (DARPA), has announced its intention to assist members of the North Atlantic Treaty Organization by implementing blockchain solutions. With 29 member countries spanning Europe and North America, communications among member nations must span borders and, because of the United States' participation, the Atlantic Ocean.

The Proposals for NATO blockchain applications include streamlining and closely tracking payments and goods transfers between members and aid recipients, decentralizing military logistics in a secure manner, and the general sharing of information between members in a way that is easily accessible, tamper-proof, and secure.

The military's supply chains, cybersecurity, and in-field, as well as inter-branch communications, are positioned to benefit from several facets of blockchain technology. **High-level blockchains are known for their security, as they can alert those in charge of security to potentially hostile anomalies in the system and limit the damage incurred.** The blockchain may not be a prevent-all solution, but we know that it is a more advanced launching point for security infrastructure than centralized fail points.

ABOUT DISPERSIVE

Dispersive provides programmable networking for mission-critical solutions. Our radically different, 100% software approach to networking delivers new levels of security, reliability, and performance and provides a foundation for innovation and transformation across industry verticals. Inspired by battlefield-proven wireless radio techniques, the Dispersive™ Virtualized Network dynamically splits session-level IP traffic at the edge device into smaller, independent and individually encrypted packet streams. Our programmable networking enables partners to connect digital businesses securely, products, and technologies end-to-end across any network infrastructure, including the public Internet.

https://www.dispersive.io

ABOUT PULSE LAB

Pulse Lab is a blockchain-focused accelerator and advisory shop providing expert consultation to startups and enterprises in technology, network construction, and governance for paradigm-shifting projects.

https://pulselab.io/

ABOUT THE SILICON VALLEY BLOCKCHAIN SOCIETY

SVBS is a global, invite-only, private, member-driven network of global investors and global deal flow in the decentralized ecosystem. The SVBS platform is entirely focused on bringing Institutional Capital, Angels, Family Offices, Corporate & Venture Capital and cross-stage expertise in Technology, Governance, Policy, Markets, Legal, Finance, and Marketing to the long-term future of decentralization.

http://svbsociety.com/

To learn more about how Dispersive Networks can help secure enterprise blockchain-based and distributed ledger systems and assets, call 1.844.403.5850.

White Paper

Securing Enterprise Blockchain with SDN

dispersive™

13560 Morris Road, Suite 3350, Alpharetta, GA 30004 | 1.844.403.5850 | dispersive.io