BDAP™ (Blockchain Directory Access Protocol™): A Decentralized Protocol for Resource Hierarchy Management and Data Storage

Disclaimer

Disclaimer: BDAP™ and its associated crypto assets (pShare™. pSign™, NoID™, etc) are currently being supported and developed by Duality Blockchain Solutions® LLC, whose website can be found at https://duality.solutions/ . This technical white paper is provided "as-is" and should be used for informational purposes only. In no event will Duality Blockchain Solutions® LLC be held liable in any way to any person or entity for use of, a reference to, or reliance on this white paper or any of the content contained herein.

Abstract

The ability to securely store, share, and manage data is a fundamental requirement for any modern enterprise. Unfortunately, the majority of solutions that address these needs force users into a trusted relationship with remote servers. End-user data housed on remote, centralized servers is at the very least subject to data mining, or in the worst-case scenario, subject to a data breach. Blockchain Directory Access Protocol™(BDAP™), is a platform that resolves these issues by providing a decentralized mechanism for resource hierarchy management, data sharing, and data storage which leverages a distributed ledger and database architecture. These distributed architectures result in trusted and fault tolerant solutions which can be quickly deployed and scale indefinitely.

1 Introduction

The centralization of data and online services has resulted in an ecosystem which provides many opportunities for malicious entities to steal private data, propagate identity theft, and generally wreak havoc on the victims of these breaches. Trusted third party servers can store passwords, private keys, and other valuable data which has proven to be a high-value target for hackers. There are many examples of these types of data breaches, one of which was a breach of Dropbox which resulted in 68 million Dropbox user's emails and passwords being exposed. As of September 7th, 2016, the data was for sale on the darknet for two bitcoins [1].

This centralization has forced internet users into relationships with servers which are not under their control. Key considerations such as threat mitigation, OS maintenance, and hardware maintenance are outside of the direct influence of the users. In order to balance this lack of trust on the internet, protocols such as HTTPS have been leveraged to encrypt all data between a server and a client by using server certificates. These certificates provide the keys used to encrypt the server-client data exchange and are also used to validate the authenticity of the server itself. “Trusted” Certificate Authorities are responsible for issuing server certificates, but unfortunately, the trust that is supposed to be generated by these centralized Certificate Authorities is not sufficient, as evidenced by the ‘mistaken’ issuance of certificates used to validate various Google sites [2]. Trusting a centralized service provider such as Yahoo can result in negative consequences in a much more straightforward manner, such as when every single Yahoo account was breached; names, email addresses and even passwords were stolen[3].

Another result of centralization is the unauthorized or obfuscated mining and sharing of user data stored on remote servers. This has been clearly demonstrated recently by the exposure of the data sharing practices of Facebook [4]. Over-privileged centralized accounts, coupled with internal actors can be problematic as well. Together, they can account for approximately 40% of data breaches. According to the 2017 Verizon Data Breach Investigations Report, 25% of breaches involved internal actors and 14% involved privilege misuse [5].

Not only is data subject to malicious actors, but critical internet services can be taken offline by attacking centralized servers. Through a DDoS attack on DNS servers in 2016, many large internet sites and services were taken offline [6]. This kind of outage can cost millions to affected businesses.

Centralization of servers and services requires administration and hosting resources. The complexity and cost of setting up and maintaining a directory access protocol to manage your enterprise can represent a large percentage of any IT department’s budget. Even open protocols, such as Lightweight Directory Access Protocol (LDAP), require centralized servers and skilled administrators to implement and maintain them.

1.1 Blockchain

In order to address some of the concerns associated with centralized and trusted service architectures, decentralized and distributed applications have begun to become prevalent. Distributed applications are applications that allow the users of a network to share tasks, and the resources required to complete those tasks across a network [7].

Blockchain technologies are one type of distributed technology which has the potential to help solve many of the problems associated with more traditional, centralized applications. Blockchain technologies leverage a peer-to-peer architecture, where each of the computers on the network can store, read, and write to a full copy of a shared public ledger (the “blockchain”). This ledger can track various transactions between participants of the blockchain in a way that is immutable, auditable, permissioned, encrypted, and distributed among all the servers, or nodes, of that blockchain [8]. Further, consensus algorithms are used to reach agreement on transactions and between nodes on a blockchain, rather than a central authority driving change and administration. A decentralized ledger can also be used to provide support that helps operate and automate business processes, applications, and services. However, currently, blockchain is difficult to implement and is not well understood [9].

1.2 BaaS (Blockchain as a Service)

To respond to the potential of blockchain technologies, while realizing the current implementation complexities involved in leveraging this potential, Duality Blockchain Solutions®, LLC, has developed BaaS, or Blockchain as a Service. BaaS brings blockchain technology to non-blockchain businesses, solving critical privacy and security issues for companies while lowering their overhead and risk of unauthorized data access. Duality® is able to accomplish this by leveraging the decentralized blockchain of Dynamic™ [10]. As a function of BaaS, Duality® will set up and maintain blockchain connected nodes for businesses across numerous industry sectors to help automate business processes, add security, and lower costs. A change from the client/server architecture to a decentralized and distributed P2P architecture can help reduce cost, reduce downtime and increase efficiency. The client/server architecture requires an expensive system and security administrators with elevated permissions. Administrators with elevated permissions can be hacked or leak private/confidential data. Instead of using administrators, BaaS uses permissionless consensus mechanisms to make sure transactions follow the rules and can be trusted. Blockchain services prevent tampering and others can validate the authenticity of a transaction without trusting a third party’s database. By shifting those tasks to BaaS, Duality® can eliminate the administrator(s) vulnerability and reduce system total cost of ownership and risk. BaaS shifts the model and charges fees for services instead of having manual system admins. An API and SDK with smart contracts allows others to write robust decentralized or distributed P2P applications without a third party authority.

1.3 BDAP™(Blockchain Directory Access Protocol™)

BDAP™, or, Blockchain Directory Access Protocol™, is a platform that provides a decentralized mechanism for resource hierarchy management, data sharing, and data storage. BDAP™ adds a layer of resource hierarchy comparable to LDAP. It provides a distributed database and account linking to our primary blockchain of Dynamic™. This makes it possible to develop core information systems from a hybrid public-private blockchain. The hybrid design allows both anonymous and identified (permissionless and permissioned) nodes to connect and share data privately and securely without a third-party intermediary. BDAP™ accomplishes this is by managing user accounts, group accounts, links between objects, audits, certificates, sidechain parameters, checkpoints, and identity records on its blockchain. BDAP™ manages accounts similar to LDAP but also stores linkages between accounts. The BDAP™ resource naming model mirrors that of the Internet, using fully qualified domain names (FQDNs), and will automatically create a unique ID for every object on the blockchain. BDAP™ is currently being registered and will have it’s own root level OID which it can use to assign child OIDs.

BDAP™ will facilitate both the creation of BaaS solutions that Duality® provides, such as pShare™ and pSign™, and will also allow third-party developers to build further groundbreaking BaaS applications for varied purposes, offering services such as VoIP, video streaming, advice forums and new methods to further lower business costs. The Duality® API and SDK will give developers access to BDAP™ objects and Distributed Hash Table (DHT) storage so they can write their own distributed applications or dApps. dApps and services are more resistant to DoS and DDoS attacks because they are distributed without a single point of failure. Application developers can isolate their application and increase performance by using a BDAP™ sidechain who’s sole task is to host your dApps.

1.3.1 BDAP™ Underlying Technology

Like many blockchain projects based on the Bitcoin UTXO model, BDAP™ leverages OP_RETURN transactions so it doesn't bloat the unspent transaction database. BDAP™ leverages Bitcoin’s OP_RETURN transactions to store data on a blockchain but increases the maximum allowed size to give us room to store more data and pointers. OP_RETURN is a way of storing arbitrary data on a blockchain without bloating the UTXO database which is needed in memory to process transactions. Currently, user, group, link, audit, and sidechain transactions are all supported using OP_RETURN in BDAP™ v1.

BDAP™ leverages the Dynamic™ primary blockchain, and all network-wide functionality is facilitated at this level. Dynamic™ makes use of special collateralized, full-nodes called Dynodes™ to help secure and support the network at the primary blockchain level. However, BDAP™ is able to facilitate applications which can scale indefinitely and handle almost any business need by leveraging sidechains and distributed hash tables (DHTs).

A sidechain is a blockchain which is defined for one specific use-case but is logically separated from the primary blockchain to perform a specific business function [11]. The federation BDAP™ has with sidechains adds scalability by logically dividing the network into separate domains that perform different functions. All sidechains can communicate using data stored on the primary blockchain. The primary blockchain serves as the intersection for all BDAP™ sidechains. Further, BDAP™ sidechains create a recursive layer as they can have their own sidechains as well.

A distributed hash table (DHT) is a class of a decentralized distributed storage system which provides lookups similar to a hash table. Key/value pairs are stored in a DHT, and any participating node can efficiently retrieve the value associated with a given key. The responsibility for maintaining the mapping from keys to values is distributed among BDAP™ nodes in such a way that a change in the set of participants causes a minimal amount of disruption. This allows a DHT to scale to extremely large numbers of nodes while being able to handle continual node arrivals, departures, and failures at the same time [12]. DHT tables can provide a robust infrastructure for the development of complex services, such as the ones BDAP™ provides. BDAP™ leverages the Kademlia DHT; this type of DHT provides robust resistance to attacks like denial-of-service attack via its ability to recover itself. BDAP™ leverages the fully collateralized Dynodes™ of Duality® to host these DHTs.

Lastly, Duality® has developed The Fluid Protocol™ to handle self-regulation, arbitration features, and voluntary governance without going through contentious hard forking scenarios [13]. Duality® uniquely understands the shifting needs of the market, and the Fluid Protocol™ is the solution to address those needs. The Fluid Protocol™ is a mechanism to change the consensus rules of the Dynamic™ blockchain, to enforce self-regulation, change the reward amounts for Dynode™ holders and miners, and respond to arbitrations (account revocation, etc).

2 BDAP™ System Architecture

2.1 Dynamic™ (DYN) Blockchain

Dynamic™ (DYN) is based on Satoshi Nakamoto's Bitcoin. Bitcoin is a peer-to-peer electronic cash system which leverages a distributed blockchain to manage its transactions [14]. However, with DYN, Duality® has enhanced the Bitcoin blockchain with many improvements which address existing issues, increase performance, and extend functionality to support the BDAP™ platform. One enhancement to the blockchain is the use of OP_RETURN transactions to create data objects on the blockchain. This allows DYN to log these transactions without bloating the UXTO database.

Unlike traditional blockchains, Duality® has increased the size for BDAP™ transaction OP_RETURN data. Solutions that use Bitcoin for OP_RETURN are restricted to 82 bytes, but DYN has increased this to 2048 bytes for data, plus 3 bytes for the script operation codes.

Unlike most transactions on a blockchain which are immutable, OP_RETURN transactions are dead-end transactions and can be pruned when expired. Using OP_RETURN, we can manage the below data on the Dynamic™ (DYN) primary blockchain:

- Users
- Groups
- Links
- Audits
- Certificates
- Sidechains
  - Sidechain parameters
  - Sidechain asset parameters
- Checkpoints
- Identity Records
- Delegates (pointers to other accounts)
- Accounts (similar to LDAP)

Not only does BDAP™ allow for the management of accounts through OP_RETURN transactions, but it also can store linkages between accounts. This allows for persistent, auditable, and customizable rules governing the sharing of information or the creation of groups. Specific accounts can act as identity authorities which help with matching. BDAP™ also leverages existing internet naming models and uses FQDNs (fully qualified domain names). BDAP™ will automatically create an OID for every object on its network. BDAP™ is currently being registered and will have its own root level OID and can use that to assign child OIDs as objects are added to the network.

2.2 Dynodes™

Dynamic™ is a so-called “Masternode-coin” which in practice means it has a two-layered approach to securing the network. The first layer is regular full-node instances of Dynamic™ and the second layer are collateralized full-nodes called Dynodes™. Dynodes™ require a user to hold 1000 Dynamic™ up as collateral, and users who run Dynodes™ are rewarded with tokens for running this network service.

Dynodes™ collateralize a fixed amount of funds (1000 DYN) and dedicate their public internet address, CPU, memory, and bandwidth to the network for a reward. Currently, there are ~1500 active Dynodes™ on the network with payments being periodically received roughly every three days. The wallet on your local machine acts as the controller wallet for your Dynodes™. We use the Dynamic™ QT wallet. It contains the Dynode collateral and can activate your cold Dynode on your virtual private server (VPS). Dynodes™ help to lay the groundwork for BaaS and are needed to propagate transactions faster and perform services like InstantSend, PrivateSend, decentralized network routing and decentralized storage for BDAP™ by hosting DHTs.

2.3 Storage/DHTs

Duality® stores mutable BDAP™ data on Distributed Hash Tables (DHTs), which are in-turn hosted on Dynamic™ Dynodes™. Dynodes™ are rewarded for hosting BDAP™ DHTs. Dynodes™ write data in the DHT after every block under their published public key and use the “proof” operation code or salt. If the data is present and valid, the Dynode is eligible for the block reward. BDAP™ DHT entries use Ed25519 public key and salt to store mutable data. Only records with a valid signature for the public key are accepted, adding an extra layer of security. DHTs typically store key, value pair hash tables which are distributed across a peer-to-peer computer network. In order to support BDAP™, Duality® has increased the max DHT entry size. BitTorrent’s Mainline DHT max entry size is 1000 bytes but we increased the DHT max size to 5120 bytes as it will be used to store encrypted and serialized JSON objects used for our dApps.

The distributed nature of DHTs provides many advantages, including resistance to attacks like denial-of-service attacks, as well as network self-recovery. BDAP™ implements the Kademlia DHT, and in a Kademlia DHT network, each active node assigns themselves a random 160-bit integer as a node ID. Nodes update their status to their nearest neighbors (other nodes with close node ids). If a neighbor drops out of the network, the other nodes closest to them take their place in the hash table and store the data that the missing neighbor should have stored. Kademlia constantly re-balances the network based on when new neighbors appear and when they drop out.

Current generation P2P networks use DHTs to look up files on a network. They are able to do this as they store the resource locations that are found throughout the network, and are responsible for adding new nodes as they are encountered on the network. The node ID serves not only as identification, but the Kademlia algorithm uses the node id as a map to help locate files and other resources. Kademlia has four messages [15].

- PING — Used to verify that a node is still alive.
- STORE — Stores a (key, value) pair in one node.
- FIND_NODE — The recipient of the request will return the k nodes in his own buckets that are the closest ones to the requested key.
- FIND_VALUE — Same as FIND_NODE, but if the recipient of the request has the requested key in its store, it will return the corresponding value.

The DHT is not only able to self recover, but it also is aided by having fast reads and slow writes. Slow writes help prevent DDoS attacks. Currently, it takes about 12-15 seconds for an add or update to fully replicate across the network. This speed is better than the blockchain and doesn't retain the old value (mutable storage) or need to store every record since each node only stores a small subset of the total database. It also has fast reads (sub-seconds), which makes it a great candidate for serving as our dApp cache layer. Currently, our 1500 Dynodes™ have a 3TB cache (including redundancy) available for our pShare™ and other primary blockchain dApps.

Although an excellent option for distributed storage, DHTs are not without their issues. Among the concerns with any distributed system is "Node churn". Node churn is a term used to reference when the nodes of a given network drop out of the network, taking their resources with them. However, BDAP™ addresses this by relying on Dynodes™ to host the network. Dynodes™ have publically routable IPv4 addresses and are fully collateralized nodes. This results in very little node churn.

Sybil Attacks (i.e., fake identities) is another concern with DHTs. We prevent Sybil-attacks by using a BDAP™ accounts' Ed25519 public key to sign new DHT entries. Our Dynodes will ignore and ban nodes that try to save DHT data that are not signed by registered BDAP™ accounts or links on our blockchain. BDAP™ accounts have registration fees with minimum registration days, so creating accounts to leach free storage from the DHT network isn't economically infeasible. Additionally, immutable DHT data storage is turned off to stop leaching free storage from the network.

A further issue one can encounter with DHTs is what is known as a "Merge-bug". DHTs self-healing properties open them up to the possibility that one DHT could erroneously merge with another DHT if a node from a compatible DHT is introduced to the network [16]. However, BDAP™ handles the merge bug by changing the DHT message structure to make it incompatible with other DHTs like BitTorrent's mainline DHT which also uses Kademlia. We have also changed the protocol signature in such a way that it is used like a magic number [17].

Duality® is constantly improving its products, and BDAP™ is no exception. Duality® is currently working on future improvements to its DHTs. These include:

- Faster write operation
- Batch read and write functions
- Improve the digest hash algorithm. Reduce message digest, infohash and node hash collisions by upgrading from SHA-1 to RIPEMD-160. We need to keep the 160-bit space but want to improve the SHA1 hash algorithm from creating collisions.
- Secure in that you can not reverse the hash to the original data
- Lower collision percentage.

2.3 Stealth Links

BDAP™ leverages stealth links to facilitate the exchange of data on the network. Stealth links function much the same way as stealth addresses. Stealth links' mechanism uses a combination of various public and private keys that are dynamic and for one-time use only. While others on the network can see a transaction getting recorded, no one other than the link participants is able to see any transaction details. As these randomly generated, one-time-use links are created for each transaction on behalf of the recipient, stealth links add an additional layer of privacy. BDAP™ stealth links use Diffie-Hellman key exchange to derive new link keys for each transaction [18].

2.4 Fluid Protocol™

The Fluid Protocol™ (Fluid) is a custom mechanism, developed by Duality®, to change the consensus rules of the BDAP™ blockchain Dynamic™. Fluid will enforce self-regulation, can change the reward amounts for Dynode holders and miners, and will respond to arbitration or attack. This allows for consensus changes without interruption to blockchain operation. Generally, it requires a hard fork to change the consensus rules for a blockchain (such as changing the rewards). With Fluid, static consensus rules change when 3 out of 5 sovereign wallet addresses sign a Fluid transaction. This is in essence, a counterparty mechanism to prevent abuse from malicious users. Fluid can ban user accounts, generate or mint new coins, change Dynode rewards, and change miner rewards. Fluid allows crucial blockchain parameter change without causing network interruptions or the need for users to upgrade their software. The Fluid Protocol white paper is available to read here.

2.5 Sidechains

A sidechain is a blockchain which is defined for one specific use case but is logically separated from the primary blockchain to perform a specific business function [11].

Sidechains are independent blockchain networks whose chain parameters are stored on the primary blockchain. BDAP™ sidechains add scalability by logically dividing the network into separate domains that perform different functions. All sidechains can communicate using data stored on the primary blockchain. The primary blockchain serves as the intersection. Dynamic™ can run both the primary blockchain and sidechain on the same computer. For public sidechains, the client would load the primary blockchain then read the sidechain parameters stored as a BDAP™ record to run another chain. Additionally, BDAP™ sidechains can create a recursive layer via their own sidechains.

Sidechains also help support BDAP™ account management. With BDAP™, end users control permission instead of centralized domain administrators. By default, all sharing is turned off. BDAP™ domain owners invite users to their sidechain applications, but unlike current models which leverage central administration, domain owners can’t change the user's keys. If users prefer not to handle their keys or permissions, they can use a delegate account that will help them manage their account.

2.6 VGP™ End-to-End Encryption/Decryption

Duality® has developed Very Good Privacy (VGP)™, an end-to-end group cryptosystem library, to provide an encryption layer which goes well beyond current PGP encryption programs to protect privacy and security [19]. VGP™ is modeled after PGP cryptosystem by using public key cryptography, symmetrical encryption, Diffie-Hellman key exchange and hashing for pubkey fingerprinting. However, Duality® has made these improvements to PGP:

- Asymmetric key uses Curve25519 (256-bit elliptic curve key) instead of RSA (2,048 - 4,096-bit linear key). 256-bit keys are much smaller than 2048 bit but offer the same level of security. The 256-bit key operations are faster as well.
- Symmetric encryption uses AES-CTR instead of International Data Encryption Algorithm (IDEA). AES-CTR doesn’t use a static IV like other AES implementations.
- Uses Shake256 (which is a SHA3/Keccak derivative) for hashing the pubkey into fingerprints. PGP uses SHA1 by default but can be changed to SHA512 by the user (so SHA1 or SHA2 upgraded to SHA3+).
- A modernized version of PGP. Creates a smaller header and uses next-generation cryptography algorithms (AES vs IDEA, Curve25519 vs RSA)
- Can encrypt data for one to many recipients using a common AES key that encrypts the
- Uses Diffie-Hellman key exchange to derive the ephemeral symmetric key and ephemeral asymmetric public keys.

3 BDAP™ Use Cases

3.1 pShare™

Duality® has implemented use cases to demonstrate both potential primary blockchain application possibilities as well as potential sidechain possibilities. pShare™ is an application hosted on the Dynamic™ primary blockchain. With pShare™ (private share) you can privately share files with friends, family, and colleagues without concerns about a third party shadowing your information as conventional file-sharing providers do. pShare™ protects privacy by leveraging stealth links, along with a peer-to-peer network linked to your BDAP™ account. State of the art encryption technology gives the user exclusive authority on who participates in shared content. pShare™ integrates directly with your file explorer, is easy to use, and compatible with most operating systems. pShare™ lets you organize your network into public and private groups, with public groups stored on the blockchain and private groups encrypted on the DHT. The primary blockchain acts as a network-auditing mechanism and adds an extra layer of access security. pShare™ connects computers behind NATs and firewalls using the same VoIP technology as large communications vendors.

3.2 pSign™

pSign™ is another use case but one which leverages sidechain functionality. pSign™ provides asynchronous 'digital signing' which completes within a matter of minutes. This is in addition to a pSign™ workflow management suite bundled with document templates, libraries, and support for full automation. By implementing pSign™, infrastructure expenditure for professionals, as well as costs associated with the current workflow and digital signing, would be decreased exponentially or removed entirely. pSign™ is a sidechain application due to its needs to support email and a web browser. Because of its need for large file storage, it is better to implement those features on a sidechain so the primary blockchain does not bloat with pSign™ needs.

4 Fee Schedule

Due to Duality® not having access to your personal data or making revenue from advertising, the services, solutions, and dApps developed by Duality® utilizing BDAP™ will not be free beyond the limits of the free tier account. For example, pShare™ will allow free tier accounts and Duality® will supply the Dynamic™ needed for the initial user registration and ten links. Once a free tier account is registered, the paid DYN is burned from the supply via the Fluid Protocol™. Every free tier pShare™ account we supply Dynamic™ will cost Duality® approximately 30 DYN per year. We plan to offer paid tier accounts that Duality® will use the proceeds from to buy Dynamic™ (DYN) from the market to set up those accounts and create buy demand. However, free tier accounts have limited functionality and are meant to drive the adoption of higher tier functionality.

Duality® uses a tiered model of fees to charge for BDAP™ services. These fees will be adjustable in v2 of the Fluid Protocol™, but our current fee structure can be found online here:
https://docs.google.com/spreadsheets/d/1pZEEwei_SHS8PO8AUbBcvEFeFtBCFnEb8abxCYFfclA/edit#gid=0

5 BDAP™ Opportunities for Improvement

Duality® is continually improving on BDAP™, its services, underlying technology, and security. Here are just a few of the improvements that Duality® has in the queue:

- Compatible with LDAP, Active Directory and as a stand-alone directory server.
- Authentication adaptors for RDBMS systems like MongoDB, Redis, MySQL, PostgreSQL, Oracle...
- Biometric identification using hash data so that we do not use personally identifiable information or PII. Salted Biohashes.
- SSO, OAuth
- Web browser plugins
- Provide block hash checkpoints to help secure the Dynamic™ primary blockchain

6 Conclusion

Centralized software and data architectures are prone to attack from malicious entities, costly to maintain, and force users into trusted relationships with outside resources who may or may not be trustworthy. BDAP™, or Blockchain Directory Access Protocol™, is a platform that resolves these issues by providing a decentralized mechanism for resource hierarchy management, data sharing, and data storage which leverages a distributed blockchain and database architecture. BaaS, or Blockchain as a Service, brings blockchain technology to non-blockchain businesses and provides a mechanism for easy BDAP™ integration. BDAP™ can facilitate the development and enterprise-level use of distributed applications such as pShare™ and pSign™, which can help reduce cost, reduce downtime and increase efficiencies for any enterprise. These applications are fault tolerant and can scale indefinitely. Through the use of the Dynamic™ primary blockchain, the Fluid Protocol™, Dynodes™, DHTs, Sidechains, VGP™ Encryption, and other cutting-edge technologies, BDAP™ offers unparalleled opportunities for solutions to many of the problems created by today's centralized data and security architectures.

BDAP™, VGP™, Fluid Protocol™, pShare™, pSign™ and NoID™ trademarks pending by Duality Blockchain Solutions®.

References:

[1] K Turner, "Hacked Dropbox login data of 68 million users is now for sale on the dark Web," Sept. 2016. https://www.washingtonpost.com/news/the-switch/wp/2016/09/07/hacked-dropbox-data-of-68-million-users-is-now-or-sale-on-the-dark-web/?noredirect=on&utm_term=.8df63676f155

[2] S. Rosenblatt, "Fake Turkish site certs create threat of bogus Google sites," Jan. 2013.https://www.cnet.com/news/fake-turkish-site-certs-create-threat-of-bogus-google-sites/

[3] S. Larson, "Every single Yahoo account was hacked - 3 billion in all," Oct. 2017 https://money.cnn.com/2017/10/03/technology/business/yahoo-breach-3-billion-accounts/index.html

[4] A. MADRIGAL, "Facebook Didn't Sell Your Data; It Gave It Away," Dec. 2018 https://www.theatlantic.com/technology/archive/2018/12/facebooks-failures-and-also-its-problems-leaking-data/578599/

[5] R. Brooks, "What to Know about the Threat of Privileged Users," Oct. 2017 https://blog.netwrix.com/2017/10/19/what-to-know-about-the-threat-of-privileged-users/

[6] L. Newman, "WHAT WE KNOW ABOUT FRIDAY'S MASSIVE EAST COAST INTERNET OUTAGE," Oct. 2016. https://www.wired.com/2016/10/internet-outage-ddos-dns-dyn/

[7] J. Frankenfield, "Distributed Applications", Jul. 2018. https://www.investopedia.com/terms/d/distributed-applications-apps.asp

[8] "What is blockchain', https://www.ibm.com/blockchain/what-is-blockchain?S_PKG=CoG&cm_mmc=Search_Google-_-Blockchain+and+Watson+Financial+Services_Blockchain-_-WW_US-_-Blockchain_Exact_CoG&cm_mmca1=000020YK&cm_mmca2=10005803&cm_mmca7=9025148&cm_mmca8=kwd-305552801503&cm_mmca9=_k_CjwKCAiAqaTjBRAdEiwAOdx9xtwO4QFBV-d18WPabesi0DmWCqJ09w1Yb85IkSAbT-hdyatOZBwi_RoC6fwQAvD_BwE_k_&cm_mmca10=218832978626&cm_mmca11=e&mkwid=_k_CjwKCAiAqaTjBRAdEiwAOdx9xtwO4QFBV-d18WPabesi0DmWCqJ09w1Yb85IkSAbT-hdyatOZBwi_RoC6fwQAvD_BwE_k_|1298|34&cvosrc=ppc.google.blockchain&cvo_campaign=000020YK&cvo_crid=218832978626&Matchtype=e&gclid=CjwKCAiAqaTjBRAdEiwAOdx9xtwO4QFBV-d18WPabesi0DmWCqJ09w1Yb85IkSAbT-hdyatOZBwi_RoC6fwQAvD_BwE

[9] "What are Blockchain's Issues and Limitations?", https://www.coindesk.com/information/blockchains-issues-limitations

[10] "Dynamic™", https://duality.solutions/dynamic

[11] S.Lee, “Explaining Side Chains, The Next Breakthrough In Blockchain,” Feb. 2018. https://www.forbes.com/sites/shermanlee/2018/02/07/explaining-side-chains-the-next-breakthrough-in-blockchain/#608c31ae52eb

[12] “Distributed hash table”, https://en.wikipedia.org/wiki/Distributed_hash_table

[13] “The Fluid Protocol™”, https://github.com/duality-solutions/Documentation-and-Guides/blob/master/fluid-protocol.pdf

[14] S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System”, https://bitcoin.org/bitcoin.pdf

[15] “Kademlia”, https://en.wikipedia.org/wiki/Kademlia

[16] N. Johnson, Jun. 2008. “Nearly all DHT implementations vulnerable to 'merge' bug”, http://blog.notdot.net/2008/6/Nearly-all-DHT-implementations-vulnerable-to-merge-bug

[17] “Magic number (programming)”, https://en.wikipedia.org/wiki/Magic_number_(programming)

[18] “Stealth Address (Cryptocurrency)”, https://www.investopedia.com/terms/s/stealth-address-cryptocurrency.asp

[19] “VGP (Very Good Privacy) E2E Technical Whitepaper v1.0”, https://github.com/duality-solutions/Documentation-and-Guides/blob/master/VGP_(Very_Good_Privacy)_E2E_Technical_Whitepaper.pdf