XYO Network: Security Risks and Mitigations

Arie Trouw *, Andrew Rangel, Jack Cable

February 2018

---

1 Introduction

The XYO Network is a trustless and decentralized cryptographic location network that utilizes zero-knowledge proofs to establish a high degree of certainty regarding location verification. A primary concern for the XYO Network, like with all decentralized and trustless entities, is the security of the system. Vulnerabilities include, but are not limited to: design/architecture flaws, coding errors, incorrect economic motivation, and social engineering. The primary focus of this document pertains to design/architecture flaws and economic motivation.

---

2 Technical Considerations

2.1 Summary

This paper addresses high level concepts in regards to potential attacks against the XYO Network. Due to the fact that the network utilizes a trustless system, it is assumed that all participants in the network are vulnerable (e.g. Sentinels, Bridges, etc.). This section details some of the known protocol-level attacks along with industry standard safeguards against them. All other attacks assume the devices in the system are compromised.

2.2 Bluetooth

Most Bluetooth devices utilize a "Long Term Key" pairing setup that establishes a PIN used for encryption. If the key is discovered through an interception of the pairing process, all future traffic could easily be decrypted. There are tools that exist that could brute force the PIN. Even well-established schemes that establish a password outside of the protocol are usually executed in an unencrypted manner. This allows for multiple attack vectors to access the protocol. In addition, devices could be easily sourced to expedite these approaches.

In order to prevent attacks of this nature, white-listing MAC addresses can prevent unauthorized devices from communicating with the Sentinels and Bridges. Another way to

*XYO Network, arie.trouw@xyo.network

counter these attacks is to require a user to physically press a "reset" button in order to pair the device, which would prevent attacks from users who do not have direct physical access to the device.

2.3 Over the Air (OTA)

Sentinels need the ability to perform "Over the Air" (OTA) updates. OTA updates allow for quick patches in order to improve the stability and security of the device. A downside of this feature is the possibility of an attack that spoofs this update and appends malicious code.

2.4 Hardware

The devices on the XYO Network are physically dispersed in a wide range of locations throughout the globe. This means that there exists an ongoing potential to physically comprise a device. This is an integral reason for the XYO Network to be a completely trustless network. The entirety of the system relies on complex algorithms that carefully and diligently parse the history and content of the data flowing into the system. Any data that doesn't pass as high-scoring, long-chain data is disregarded and the offending devices are penalized.

---

3 Poison the Well Attacks

3.1 Summary

A Poison the Well Attack occurs when a malfunctioning or malicious party creates and injects corrupted data which decreases the overall accuracy and/or certainty of results generated by the system.

3.2 Motivation

In a Poison the Well Attack, the bad actor's goal is to disrupt or *poison* the data that is being sent to a particular Sentinel or Bridge. Achieving this would allow them to cause both short-term and long-term economic disruption. Given that the XYO Network is a trustless system, there is a low tolerance for this type of bad data to enter the network.

While there is no direct gain for the bad actor, there exist benefits in the disruption and/or tampering of other peoples' data *reputation*. Suppose the XYO Network was employed to track the location of parolees in order to report any location-based violations of parole terms. If this were used to monitor the amount of time a serial DUI offender spends at a bar, an offending parolee could Poison the Well by feeding a bar-based Bridge bad data until it is knocked off the network. The delinquent could then violate the terms of their parole and consume alcohol at the bar for as long as he or she pleases. Even if the provided data reported the offender as being at the bar's location, the poisoned data could reduce its certainty to the point that it is rendered invalid.

3.3 Technical Analysis

Location data of a Sentinel could be affected by GPS jammers or illegal radio frequency transmitters that are designed to interfere with authorized radio communications. GPS spoofing devices [1] have the ability to send false data to GPS radio receptors in order to falsify location.

Sentinels communicating via Bluetooth present another vector for this type of attack. There are various methods in which a Bluetooth device could be spoofed into sending bad data [2]. While the private keys created by the XYO Network are immediately deleted, it is possible that a device could listen to the communication between a Sentinel and a Bridge and copy the data that is sent. This thief could then send bad data acting as the Sentinel and begin to poison the data the Bridge sends to the Archivists.

3.4 Protocol Mitigation Strategies

While active, a GPS jammer can be easily recognized due to the pollution it causes to the general area it is targeting. For example, any cell phone user in the targeted area would experience a sudden block out of many of the apps they use. It would only be a matter of time before multiple parties confirm similar issues and are able to confirm a jammer is the culprit. Given that this type of disruption is highly detectable combined with the fact that the FCC has explicitly ruled that invoking jammers is illegal [5], the high risk associated with this type of attack renders the likelihood of its occurrence to be low. Even so, there are sophisticated GPS anti-spoofing techniques that are currently being developed both at the hardware and software levels for added security [1].

In addition to these safeguards, there are current technologies and strategies that enable us to protect against Bluetooth spoofing and disruption, such as authenticating link keys with secure connections. [3]

3.5 XYO Network Mitigation Strategies

The Archivist network is a competitive network that returns verified data upon being queried by Diviners. At the point at which Archivists receive data (detailed in yellow paper), the network begins to prune bad data. The relaying of the information stored on the chain back to the origin allows for the detection of recently added bad data, even with spoofed information on a long chain. Each Archivist also cross-checks the other Archivists' data to build a valid consensus for the network. Due to the fact that Archivists get paid, along with Bridges and Sentinels, inherent cryptoeconomics suppress attempts to poison lower-level components.

3.6 Conclusion

Considering an Archivist pulls data from a wide geographical region and there is a necessity for it to be physically located somewhere in order to poison that region, this type of attack would result in the attacker being punished by the network. This is what makes an attacker economically disincentivized to conduct such an attack on the XYO Network.

---

4 Assassination Attacks

4.1 Summary

An Assassination Attack is defined by a malicious actor attempting to discredit a node (character assassination) or render another node non-functional (technical assassination).

4.2 Motivation

In an Assassination Attack, an attacker is motivated to undermine the reputation of legitimate nodes in order to boost the relative credibility of other nodes controlled by the attacker. As the reputation of Sentinels on the XYO Network is fundamental for a functioning network, it is crucial that the reputation of nodes cannot be easily manipulated.

Consider a situation where an attacker attempts to broadcast false location information on the XYO Network (detailed further in the Force Field Attack). In this case, the attacker must first target individual nodes to harm their reputation. One method in which this could be accomplished is via selective signing, where an attacker selectively provides false information to a legitimate Sentinel (rendering its data an outlier) in order to make the node less consistent with other nodes on the XYO Network. This causes the Sentinel's reputation to be lowered relative to other nodes on the network.

Additionally, an attacker may engage in a technical assassination of a node, such as physically destroying a device. These types of attacks are also made in attempts to falsify location information on the network and result in non-functional devices.

4.3 Technical Analysis

An Assassination Attack on a Sentinel requires an attacker to deploy at least one device to selectively communicate with the target Sentinel. Since other devices on the network do not generate signatures with the malicious node, the malicious node is only visible onto the target node.

To Bridges, external to the network, the information broadcast by the target node is inconsistent with the rest of the network. This has the effect of the target node losing reputation with respect to the rest of the network, which are consistent in not recognizing the malicious node.

4.4 Protocol Mitigation Strategies

Fundamental to the protection against an Assassination Attack is the establishment of punishing a node's reputation if it engages in selective signing. In this scenario, the malicious nodes engage in selective signing in order to make themselves appear invisible to other Sentinels on the network.

Establishing a reputation of each Sentinel according to its consistency with the rest of the network makes it possible to punish nodes that engage in selective signing. A reputable node may issue a query to a less reputable node on the network. If the less reputable node is legitimate, it would be in its best interest to sign the query and make itself visible to the network, increasing its reputation. Thus, if a node were to practice selective signing, the more reputable node can broadcast that the malicious node refused to sign its query. This practice can not be exploited in the case where a node actually does sign the query, as the legitimate node can then broadcast its signature to disprove the selective signing accusation.

The act of punishing selective signing within the XYO Network mitigates character assassination attacks, as each Sentinel has a defense mechanism for receiving inconsistent information.

4.5 XYO Network Mitigation Strategies

Establishing a reputation for each Sentinel discourages nodes from engaging in selective signing. This mitigates character assassination attacks by making any Sentinel on the network punishable for selective signing. Physical assassination attacks (e.g. destroying a device) are harder to prevent at the network level, but the XYO Network is resilient to attacks that target single devices.

4.6 Conclusion

The establishment of a reputation system allows Sentinels to enforce each other's good standing and eradicate bad actors. This is how the XYO Network mitigates Assassination Attacks.

---

5 Deception Attacks

A Deception Attack occurs when a malicious actor tries to pass off incorrect, yet valid data to be used in the system for personal gain.

One form of a Deception Attack occurs by Multi-Chain Forging, where an attacker maintains multiple versions of their own chain that could essentially exist in multiple places at once.

5.1 Motivation

An attacker could falsify information by forking their own location chain. This could be accomplished by sending the private key for one chain link, which is generated during the creation of new local blocks, to one or more colluding adversaries in different areas. This allows for continued creation of new location chains that branch from the same point of origin.

An attacker could benefit from spreading false information about their location in situations where accuracy of location is imperative. Take for example the intent to establish an alibi to attest that the attacker was present at a specific location at a given time. By having multiple chains, the attacker could selectively report only the chain carrying information is most advantageous to them as an alibi.

5.2 Technical Analysis

A Deception Attack is increasingly difficult to execute as a chain grows longer. As time progresses, information from a particular node is broadcast across the XYO Network. This means any feasible attack would allow, at most, a few small changes to a chain at a given point in the past.

This process does not completely diminish a potential for an attack. While syncing with a Bridge, a malicious Sentinel could choose one of its forked chains to share with the Bridge. Since both chains are valid, the Bridge and other devices upstream cannot immediately conclude that the chain has been forked. Instead, it is essential for nodes to cross-check with records of communication with other Sentinels on the network to verify that the node has not existed in multiple locations at once.

5.3 Protocol Mitigation Strategies

The XYO Network, by nature, can detect Multi-Chain attacks. Any long-term fork of a node's chain will be inconsistent with the general consensus of the network. In order to prevent small modifications, when the integrity of location data is paramount, a user may wait for additional confirmations from Archivists containing signatures from distributed nodes. As time progresses, any discrepancies resulting from a forked chain will become apparent.

5.4 XYO Network Mitigation Strategies

Data is distributed throughout the Archivists that contain signed ledgers of communications between Sentinels. In practice, even slight (though valid) modifications of an existing chain are detectable. If a Sentinel attempts to perform a Multi-Chain attack, other nodes with conflicting histories can broadcast the conflict to the network. As a result, the reputation of the rogue Sentinel will drop, forcing all its chains to be removed from the network.

Thusly, XYO Network is designed to enable the cross-checking of these communications as a safeguard against these types of attacks.

5.5 Conclusion

The data redundancy in the XYO Network deters attempts to broadcast inconsistent data by lowering the reputation of any offending Sentinel to a level that removes it from consideration in the network.

---

6 Same-Machine Sybil Attack

A Same-Machine Sybil Attack occurs when a malicious actor creates multiple nodes from a single machine. Since devices on the XYO Network aren't assigned unique IDs, this is easily achievable. The malicious actor reinforces reputation by signing packets between the simulated nodes to portray the nodes as organic and pure. The attacker then lets the nodes each communicate with different groups of nearby nodes such that each simulated node keeps different information in their Proof of Origin Chains. This results in all simulated nodes acquiring high Origin Chain Scores. This attack allows malicious actors to inexpensively mass-produce nodes that can be used to conduct Sybil attacks on a local or even global network.

6.1 Motivation

An attacker may seek to engage in a Same-Machine Sybil Attack to inflate influence over a particular region. By creating multiple fake nodes from the same device, the barrier to execute a Sybil attack is lowered. It is much easier for an attacker to create many fake devices on one machine than create many malicious devices.

6.2 Technical Analysis

It is not difficult to spoof a Bluetooth device's information in order to appear indistinguishable from the device [4]. Thus, an attacker could create multiple devices from one computer that act and appear as separate devices.

Once a number of virtual Sentinels have been created, an attacker can operate the Sentinels as if they were physically distinct. The Sentinels would appear to be organic and proceed to sign information related to other Sentinels in their proximity. Additionally, an attacker could create a virtual map of devices that are reflected in the signatures of the virtual Sentinels.

6.3 Protocol Mitigation Strategies

The key to defending against a Same-Machine Sybil Attack is the ability to detect duplicate data by analyzing signal strength. A computer running many virtual Sentinels would appear to have the same RSSI for each Sentinel. As a result, to an external Sentinel, each virtual Sentinel operating on the computer would appear to be close to each other (provided a certain fluctuation in signal strength). In order to prevent this type of attack, it is important for a legitimate Sentinel to detect bundled devices and treat their information as a single node.

6.4 XYO Network Mitigation Strategies

The XYO Network's primary indicator for detecting Same-Machine Sybil Attacks is Bluetooth signal strength (RSSI). This is a two-way metric which can be agreed upon by two nodes. As a result, a node running a Same-Machine Sybil Attack will appear to have the same signal strength for each of its virtual nodes. De-duplication of node data is pruned by Archivists, causing all virtual nodes to be treated as a single node. This renders a Same-Machine Sybil Attack ineffective in representing one machine as several virtual nodes.

6.5 Conclusion

The XYO Network's detection of Bluetooth signal strength coupled with its ability to de-duplicate data mitigates an attack from a machine that creates a cluster of virtual nodes by treating the cluster as a single node.

---

7 Force Field Attacks

A Force Field attack combines an Assassination with a traditional Sybil attack in order to provide false data to a network. The attack is twofold: an attacker feeds inconsistent

information to legitimate nodes while simultaneously allowing the attacker's network of nodes to serve as a consistent network for outside observers.

7.1 Motivation

This approach takes the form of a local Sybil, where the attacker aims to completely control the authority of a certain physical location. However, a pure Sybil attack on the XYO Network would require a large number of distributed devices with extensive histories in order to outnumber the existing reputable nodes. To circumvent this obstacle, a Force Field Attack employs a hybrid approach, which first targets the reputation of existing nodes via Assassination Attacks in order to create inconsistencies between legitimate nodes.

Consider a situation where an attacker wishes to have complete authority of a certain local region. Employing a Force Field Attack, the attacker could first flood each legitimate node with inconsistent information. The reputation of these nodes on the network would consequently decrease, lowering the reputation qualification barrier. With this reduced barrier, an attacker could supply their own network of devices that outnumber the lowered reputation of legitimate devices, establishing singular authority for the targeted region.

7.2 Technical Analysis

In order to render an existing network inconsistent, an attacker utilizes selective signing in order to decrease the overlap between legitimate nodes. This could be done by bringing malicious nodes into the local network, and then allowing each node to only communicate with particular devices on the network. Each legitimate Sentinel selected would broadcast the location of the malicious node it communicates with, while the malicious node remains invisible to surrounding Sentinels. On a large scale, this would cause each Sentinel to have a vastly different interpretation of the state of the network. To an outside source, such as a Bridge, the reputation of each node would be lowered.

Once this is accomplished, an attacker could take advantage of the reduced reputation of the entire system in order to inject their own network of Sentinels. It is possible that these devices have already existed on the network, they would simply become more significant as the reputations of other Sentinels are lowered.

This method of attack is contingent on the number of existing nodes in the region and becomes increasingly difficult as this number grows.

7.3 Protocol Mitigation Strategies

Similar to prevention of Assassination Attacks, mitigation of Force Field Attacks relies on the punishment of selective signing. A Force Field Attack employs selective signing with a cartel of malicious nodes in order to make targeted legitimate nodes inconsistent with the XYO Network.

Having reputable Sentinels poll less reputable nodes for signatures and reporting nodes that refuse to respond diminishes the ability of nodes to engage in selective signing.

This makes a Force Field Attack much more difficult to execute, because any reputation built to execute the attack would quickly dissipate after engaging in selective signing.

7.4 XYO Network Mitigation Strategies

The XYO Network punishes nodes that attempt selective signing for not conforming with the rest of the system. This boosts the incentive for nodes to respond to signing requests and contribute data to the XYO Network. Incompliant nodes lose credibility in the form of lowered reputation, causing the Assassination component of a Force Field Attack to be economically inviable. This reduces a Force Field attack to a traditional Sybil attack, which requires an inordinate amount of devices and computing power.

7.5 Conclusion

The resulting cost to a Sentinel's reputation in a Force Field Attack on the XYO Network renders the attack economically impractical.

---

8 Teleportation Attack

8.1 Motivation

A Teleportation Attack occurs when an attacker is able to falsify their location by "teleporting" to another location through the network. If a smart phone or Bluetooth beacon is utilized as the Sentinel that provides an attacker's location data, an attacker could falsify their location by sending their Sentinel with someone else. If the network were utilized to establish an alibi, a bad actor could swap their Sentinel with someone else in order to falsify their reported location.

This type of attack could also be achieved at the software level by an attacker sharing their private key with one or more individuals. If the network was employed to verify hotel reviews, it would only allow people to leave reviews that had trusted, on-chain history. A bad actor could remotely share their private key with an individual at the hotel and could appear as if they were located there without being in physical proximity of the area.

8.2 Technical Analysis

If the private key is provided to the user, it could be shared to create a spoofed device that appears as that users device. The utilization of Software Defined Radio would allow eligible parties to appear as any specific device on the network, provided it is associated with that device's private key. This would nullify attempts to validate a user's location. This could also affect data on the blockchain, as it is theoretically difficult to discern legitimate device travel from a Teleportation Attack.

8.3 Protocol Mitigation Strategies

Detection strategies against this type of attack are complex due to the natural breaks in the chain. For example, if a phone is utilized as a Sentinel and it is turned off, it is not in communication with the network until it is turned back on. Gaps in information being sent require a sophisticated algorithm to distinguish natural gaps from potentially bad data points that must be penalized.

8.4 XYO Network Mitigation Strategies

The feasibility of a Teleportation Attack falters at the point where the Archivists are able to share information with each other and verify data viability. The number of eligible devices is further reduced upstream on the Network, where it is realistic for servers to compare data across large geographic areas. This allows Diviners to observe bad data in the form of duplicate locations and Teleportation, which can be filtered and punished with use of an algorithm.

8.5 Conclusion

While a Teleportation Attack is difficult to determine at the protocol-level, higher-level servers on the XYO Network, such as Archivist, enables detection and punishment of malicious data on the Network. Information sharing between these servers will continually build and append trusted information in order to filter bad data from the system.

---

9 Stealth Attack

A Stealth Attack is defined by a device masking itself from the network. Various use cases of the XYO Network require the devices on the network to have a solid chain history.

9.1 Motivation

There is little incentive for a malicious user to conduct a Stealth Attack on the XYO Network. The network aims to provide certainty that something exists in a given location, not prove *everywhere* it has been. This is an important distinction, as the protocol-level data can be inaccurate as nodes are not trusted.

Even so, an offending user could strategically turn on and off the location services of their phone or beacon to create bad chain data that would otherwise appear valid. This would allow them to essentially hide themselves from the network when they do not wish to report data and re-appear to the network when it is advantageous to them.

9.2 Technical Analysis

A Stealth Attack could be achieved by turning off a device on the network. A more complicated approach could be to employ a Faraday cage that hides a device from the network. A non-physical approach to this type of attack could be persisted through Denial of Service Attacks.

9.3 Protocol Mitigation Strategies

Action against Stealth Attacks can be complex due to the ability of Bluetooth and other devices to be easily disconnected from the network. The main strategy to alleviate this vulnerability is the implementation and usage of a strong software layer that penalizes Sentinels and Bridges that broadcast broken chain data. Detection capabilities will learn and grow over time as the algorithm gets better at understanding the subtle differences between valid and invalid data.

9.4 XYO Network Mitigation Strategies

A gap in a node's history will be immediately suspicious in use cases that require a continuous Proof of Location on the XYO Network. When data reaches the Archivists, it undergoes a rigorous pruning and filtration process that can detect these gaps and punish inconsistencies. This primary feature of the XYO Network allows it to provide the most accurate location despite messy data that is inherent of the physical world.

9.5 Conclusion

A Stealth Attack is economically inviable given the use cases for the XYO Network.

---

10 Denial of Service Attacks

A Denial of Service Attack (DoS) occurs when a malicious or dysfunctional actor causes a local, regional, or system wide outage.

10.1 Motivation

An attacker may seek to disrupt the XYO Network in order to prevent it from being able to verify Proof of Location.

10.2 Technical Analysis

Due to the nature of the Bluetooth protocol, Bluetooth beacons can only connect to one device at a time. This means any device that accepts unauthenticated commands can easily be knocked off the network. This could be achieved by utilizing a mobile phone application, which would allow one device that broadcasts Bluetooth commands to do so continually with relative ease. Sending hex values to the device for given parameters, such as the "play sound" parameter on most beacons, creates a connection with that device. If this connection is established, it blocks any other device from communicating with it. This could be amplified by the use of Software Defined Radio that could run scripts to continually broadcast various hex values to any network beacon in range.

10.3 Protocol Mitigation Strategies

Bluetooth devices on the XYO Network should only accept authenticated commands or utilize a MAC address white-list. Reducing the number of write-authenticated commands minimizes access to this attack vector.

10.4 XYO Network Mitigation Strategies

The XYO Network is comprised of users who run Archivist and Diviner servers. Both of these components share information and validation with their peers. This allows a query to select from any "stack" of components to retrieve an answer. While it is possible to deny a small portion of the network service at the protocol level, the breadth and scale of the network makes this economically inviable.

10.5 Conclusion

Due to the distributed nature of the XYO Network, the network remains functional despite an attempted Denial of Service Attack. As a DoS requires heavy computing power and physical access to attack an entire stack, targeting even a small portion of the XYO Network is expensive and economically illogical.

---

11 Acknowledgements

This red paper is a security corollary to the XYO Network white paper and XYO Network green paper. We thank Christine Sako for her attention to detail and application of best-practices in her review of this work.

References

[1] Jafarnia-Jahromi, Ali. Ali Broumandan, John Nielsen, and Gerard Lachapelle. *GPS Vulnerability to Spoofing Threats and a Review of Antispoofing Techniques.* `https://www.hindawi.com/journals/ijno/2012/127072/cta/` International Journal of Navigation and Observation, Alberta, Canada, May 2012.

[2] Padgette, John, John Bahr, Mayank Batra, Marcel Holtmann, Rhonda Smithbey, Lily Chen, and Karen Scarfone. *Guide to Bluetooth Security.* `http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-121r2.pdf` U.S. Department of Commerce, National Institute of Standards and Technology, May 2017.

[3] Dunning, JP. *Breaking Bluetooth by being bored.* `https://www.defcon.org/images/defcon-18/dc-18-presentations-/Dunning/DEFCON-18-Dunning-Breaking-Bluetooth.pdf` DefCon, August 2010.

[4] haxf4rall. *Spoofing a Bluetooth device.* `http://haxf4rall.com/2016/05/11/spoofing-a-bluetooth-device/` May 11, 2016.

[5] Chief, Enforcement Bureau. *FCC Enforcement Advisory.* `https://apps.fcc.gov/edocs_public/attachmatch/DA-14-1785A1.pdf` FCC.gov, December 8, 2014.

Glossary

accuracy A measure of confidence that a data point or heuristic is within a specific margin of error. 2

Archivist An Archivist stores heuristics as a part of the decentralized data set with the goal of having all historical ledgers stored, but without that requirement. Even if some data is lost or becomes temporarily unavailable, the system continues to function, just with reduced accuracy. Archivists also index ledgers so that they can return a string of ledger data if needed. Archivists store raw data only and get paid solely for retrieval of the data. Storage is always free. 3, 6, 7, 10, 11

Bridge A Bridge is a heuristic transcriber. It securely relays heuristic ledgers from Sentinels to Diviners. The most important aspect of a Bridge is that a Diviner can be sure that the heuristic ledgers that are received from a Bridge have not been altered in any way. The second most important aspect of a Bridge is that they add an additional Proof of Origin metadata. 1–4, 6, 8, 10

certainty A measure of the likelihood that a data point or heuristic is free from corruption or tampering. 2

cryptoeconomics A formal discipline that studies protocols that govern the production, distribution, and consumption of goods and services in a decentralized digital economy. Cryptoeconomics is a practical science that focuses on the design and characterization of these protocols. 3

Diviner A Diviner answers a given query by analyzing historical data that has been stored by the XYO Network. Heuristics stored in the XYO Network must have a high level of Proof of Origin to determine the validity and accuracy of the heuristic. A Diviner obtains and delivers an answer by judging the witness based on its Proof of Origin. Given that the XYO Network is a trustless system, Diviners must be incentivized to provide honest analyses of heuristics. Unlike Sentinels and Bridges, Diviners use Proof of Work to add answers to the blockchain. 3, 10, 11

Origin Chain Score The score assigned to an Origin Chain to determine its credibility. This assessment takes length, tangle, overlap, and redundancy into consideration. 6

Proof of Origin Chain A Transient Key Chain that links together a series of Bound Witness heuristic ledger entries. 6

Sentinel A Sentinel is a heuristic witnesses. It observes heuristics and vouches for the certainty and accuracy of them by producing temporal ledgers. The most important aspect of a Sentinel is that it produces ledgers that Diviners can be certain came from the same source by adding Proof of Origin to them. 1–4, 6–10

trustless A characteristic where all parties in a system can reach a consensus on what the canonical truth is. Power and trust is distributed (or shared) among the network's stakeholders (e.g. developers, miners, and consumers), rather than concentrated in a single individual or entity (e.g. banks, governments, and financial institutions). This is a common term that can be easily misunderstood. Blockchains don't actually eliminate trust. What they do is minimize the amount of trust required from any single actor in the system. They do this by distributing trust among different actors in the system via an economic game that incentivizes actors to cooperate with the rules defined by the protocol. 1, 2

XYO Network XYO Network stands for "XY Oracle Network." It is comprised of the entire system of XYO enabled components/nodes that include Sentinels, Bridges, Archivists, and Diviners. The primary function of the XYO Network is to act as a portal by which digital smart contracts can be executed through real world geo-location confirmations. 1–12