Crypto Assets: Extending Permissionless Innovation

Luka Jankovic and Ivan Brightly

Galaxy Digital LP[1]
{luka.jankovic, ivan.brightly}@galaxydigital.io

August 2018
Revised January 2019

Abstract. The purpose of this paper is to describe the purpose and necessity for native crypto assets to enable decentralization. We highlight key problems solved by non-centralized networks and crypto assets, including information sharing, data protection, developer alignment, and incentive structures in distributed systems.

1 Introduction

Historical innovations in how humans have created, recorded, and shared information have led to the most profound step-function changes in civilizations and societies. Information encoding evolved from cave art to symbols, the written and spoken word, and alphabets. This information encoding and transfer evolved from stories told over generations to writing, printing presses, telegraphs, and telephones. Information sharing has evolved in a similar manner. Scroll and letter carriers were the dominant method to share information for hundreds of years, until the advent of the computer and digital information in the 1900s provided an efficient and reliable way to encode and share information.

Through computers society developed the Internet: a shared, global interconnected computer network providing a variety of standardized information and communication protocols. The Internet has become our digital information highway, guided and controlled by government agencies, ISPs, and corporations. Over the past few decades, inefficiencies in the infrastructure, information rails, and applications of the Internet provided opportunities for companies to become dominant leaders in the industry. Society trusts these centralized organizations to be responsible gatekeepers and curators of the information its citizens create and share. However, these centralized entities pose existential risks to our ability to distribute and protect information. There is no guarantee that these companies will not abuse their powers and influence our access to data. As corporations mature they become forced to extract more value from their users, unlike decentralized platforms that can remain neutral and are not under similar constraints. Centralized data storage and distribution has become a centralized point of attack for malicious actors. News of security breaches of companies and organizations is commonplace, and tools to breach security measures are becoming more sophisticated. While centralization has made access to information efficient, it has also made it easier to manipulate and breach. Furthermore, the centralization of the Internet and closed networks do not incentivize or provide open source development monetization, hindering natural competitive forces and innovation.

Open networks solve many of the key issues that today's Internet faces. Shared public databases and protocols can provide efficient information creation and sharing among participants without data manipulation and single points of failure. Native compensation that aligns developers and users enhances security and allows the network to achieve consensus of the information in digital systems. Cryptography and a resurgence in cryptographic innovations provide tools to protect and verify information.

This paper is organized as follows. Section II describes a brief history of the Internet and highlights some of the developer and infrastructure problems. Section III illustrates the solutions open networks and intrinsic compensation solve. Section IV highlights the incentive structures present in crypto networks and assets. Section V concludes the paper.

2 A Brief Overview of the Internet

The original Internet was not designed to be centralized. In fact, the Internet was a project proposed by the US Department of Defense (DoD) to establish a decentralized communications network that could withstand unforeseen events and disasters so that if one part of the system fails the rest could still function. In addition, the Internet was designed to communicate using peer to peer interconnectivity without relying on a centralized hub.

The first successful message on a peer to peer network was made between researchers from UCLA and the Stanford Research Institute (SRI) using ARPANET on October 29, 1969. Though originally designed as a military project, peer to peer networks slowly evolved in the early 1980s through the NSFNET Project with the National Science Foundation (NSF) with the aim of promoting research and education through the use of an interconnected network of computers for information sharing. These early projects served as early test cases for the "Internet," of portmanteau of "interconnected" and "network."

Critical Internet protocols emerged to provide the backbone for the Internet and Web 1.0. TCP/IP (Transmission Control Protocol/Internet Protocol) was developed by DARPA (DoD Advanced Research Projects Agency) to serve as the data communication standard for the Internet. These base protocols gave the Internet application layer protocols such as e-mail, file transfer, newsgroups, web pages, instant messaging, voice over IP, and a variety of other data transfer methods. This system that would allow documents to be linked to other nodes and was the beginning of hypertext, linking information stored on other computers in the network. Users no longer needed to know the actual location or computer name to access resources through the use of Hyper Text Markup Language (HTML) hyperlinks. Websites could be accessed through these links and this linked system became known the World Wide Web.

Information retrieval and consumption grew through the advent of the browsers like Mozilla and Netscape. Microsoft's introduction of Internet Explorer (IE) in 1995 led to wider adoption of the World Wide Web and use of the Internet. Search engines provided a simple and fast way for users to retrieve information on the Internet. Browser-based search engines like Lycos, Yahoo, and Webcrawler were the first iteration of the modern-day search engines. Google appeared toward the late 1990s and became the most popular search engine. Internet Service Providers (ISPs) helped provide more content

at faster data speeds. Bundling services became commonplace. Companies mailed free CD software to encourage users to sign up, offering faster DSL and ADSL services as alternatives to dial-up. Cable companies provided high-speed Internet using cable modems that became known as broadband service. Telecom companies built the infrastructure to offer faster speeds, allowing users to download data, stream video, chat, browse active content on the web, and video conference.

The first versions of the Internet were disorganized and highly decentralized. There was no central authority and every computer was independent of each other. If one server was not working, users could always dial-up another server. However, this type of system had its disadvantages. Servers that contained the information or a user's e-mail could fail. The process was also inconvenient, because you had to dial-up to a different computer every time every so often. Internet Service Providers (ISP) entered the picture during Web 1.0 when the Internet was mainly web pages and hyperlink content. By providing the Internet as a service to users, ISPs could make using the Internet more convenient.

The commercialization and centralization of the Internet evolved together. Microsoft bundling a free Internet Explorer with its Windows Operating System starting with Windows 95 extended the Internet to Windows users and effectively killed off Microsoft's competitors. Netscape shuttered while other browsers like Mozilla were marginalized. The Internet thrived with its commercialization as network effects took hold and more users joined, allowing information to be shared and accessed. News giants established an online presence and became media outlets. Broadband Internet providers who offered bundled Internet services with telephone and cable service threatened smaller ISPs who could only offer Internet. This convergence of services led to a more centralized Internet.

Today, Internet access requires an ISP for the majority of its users. Web 2.0, characterized by user generated content and interoperability of web pages, developed alongside more dynamic content and devices. Cloud computing provided a virtual collection of servers and services to users. Commercial interests grew alongside this functionality and greater Internet use, and many social media platforms emerged. Many of these giants like Google, Facebook, and Twitter bought smaller companies and consolidated in a race for market share. Social media platforms gave themselves broad discretion over user information through lax Terms of Service, allowing them to censor, block, delete, and sell data to third parties.

The centralized Internet expanded due to the services provided by the ISPs and the popularity of Internet applications. However, the user's access to the Internet is at the mercy of the provider and platform. Many users don't have options to select from an array of ISPs given the consolidation and lack of competition. The centralized nature of Internet data also poses a security concern as single points of failure make data an easy target for hackers. Personal and sensitive information can be compromised through centralized attacks. Centralized systems can be targets for disruptive activities like DDOS attacks, service outages, and malware. ISPs and corporate platforms hold a disproportionate influence on the Internet, and consequently over the users of the Internet. Without competitive forces, these organizations have no incentive to innovate and protect private information. Traditional centralized platforms remain open to developers only in the initial stages. As soon as the platform operator's business model no longer requires third party developers it needed during early growth stages, it restricts API access and ensures that third party applications cannot compete with the main offerings. By offering a neutral and stable platform, decentralization and crypto assets offer some solutions to these problems and provide potential innovation for the future development of the Internet.

3 Permissionless Innovation

Open networks and ledgers (sometimes referred to as public blockchains) provide several solutions to many of the key problems the current Internet faces, highlighted in Table 1 below and described in greater detail in subsequent subsections.

Problem	***Solution***
Centralized information storage and communication rails can censor, delete, or abuse private information	Open, shared databases and protocols with peer to peer communication
Difficult to incentivize open source development with end users	Align developers and users with native means of exchange
Information is vulnerable to hacking or manipulation	Information can be cryptographically secured on multiple locations

Table 1: Solution Matrix

3.1 Open, Shared Ledgers & Protocols

Open databases and computer networks provide decentralized communications networks that use peer to peer interconnectivity without a single centralized hub. They provide efficient information creation and sharing among its participants without a centralized entity that can manipulate or censor the data that the participants intend to share. Furthermore, open ledgers and protocols eliminate single points of failure and mitigate the damage from DDOS attacks, service outages, and malware.

Open networks can also remove the inherent information and influence asymmetry that is present in today's Internet. Since anyone can join and contribute to the network, the development of the technological infrastructure that underpins the network is no longer limited to just the centralized hub. Furthermore, networks without geographical barriers address a substantially larger market and user base. Cross-border business activity and information can remove traditional intermediaries and create efficiencies.

3.2 Aligned Governance & Development

Open networks and blockchains with native mediums of exchanges can align developers' incentives to operate, secure, and innovate a distributed network that ultimately benefits the end user.

Open networks allow people to share and agree on virtually anything without intermediaries, providing a foundation to make social contracts based on consensus. Network consensus performs checks and balance on competing self-interests and potentially corruptible propensities. The economic incentive that aligns the keepers of the network state and users is an innovation in social accountability. Unlike traditional models of governance that is exercised through third parties, accountability in open networks is distributed and exercised by all participants. This eliminates centralized points of governance that can be susceptible to attack, corruption, or stagnation by strengthening the accountability via decentralized forms of governance.

Closed networks, such as AOL, struggled to survive because permission was required to innovate and develop. Today's open source development struggles with funding and permanent developer/user alignment. For example, TCP/IP, the critical communication protocol for the modern Internet, is maintained by the Internet Engineering Task Force (IETF). Since 1993, the IETF has served a voluntary standards development function within the Internet Society (ISOC), an international membership-based non-profit organization, to provide technical direction for the Internet in conjunction with the Internet Architecture Board (IAB), the Internet Engineering Steering Group (IESG), and the Internet Research Task Force (IRTF). The ISOC is funded through organization member fees, from companies like Cisco, Google, AT&T, Comcast, and Verizon. ISOC's budget is roughly $45 million according to most estimates, which is entirely based on voluntary donations. The current funding model is reliant on volunteer donations from Internet corporations, who may not be aligned with the end user. Evergreen funding models that align developers with users mitigate the influence rent-seeking intermediaries have, while also incentivizing innovation on the key protocols of open networks.

Many cryptographic open networks use development funds that are either funded through pre-mines or a portion of block rewards that continue to provide financial capital for research and development. Tokenized ledgers create aligned incentives and compensate developers and engineers for open-source software and projects. Furthermore, tokenized blockchains allow for

the monetization of open-source software protocols and value capture from the network.

4 Incentives

Decentralized networks pose new requirements in forging consensus: a shared version of truth. In modern networks, achieving consensus without a central repository is a challenge best described as the Byzantine General's Problem.

4.1.1 Byzantine General's Problem

Originally described in 1982, the Byzantine General's Problem is an agreement problem in distributed systems where participants on a network must agree on a single strategy in order to avoid complete failure. However, some of the involved parties may be corrupt, disseminating suboptimal (false or faulty) information.

In the Byzantine General's Problem, a group of generals each command a portion of the Byzantine army and encircle a city. The generals must decide whether to attack or retreat. Every general must agree on a path forward. If only some generals attack, the Byzantine army will lose and both the attacking and retreating factions will be defeated. Success can only be achieved through a coordinated attack or a coordinated retreat. The generals are physically separated and have to send their messages in a peer to peer manner.

The situation is complicated by the presence of malicious generals who intend to disseminate suboptimal information. The malicious generals will distribute suboptimal information and may do so selectively based on the recipient. For example, imagine five generals are voting, two who support attacking, two who support retreating, and one malicious general. The malicious general may send a vote of retreat to those generals in favor of retreat, and a vote of attack to the generals who favor an attack. The problem is illustrated in *Figure 1*.

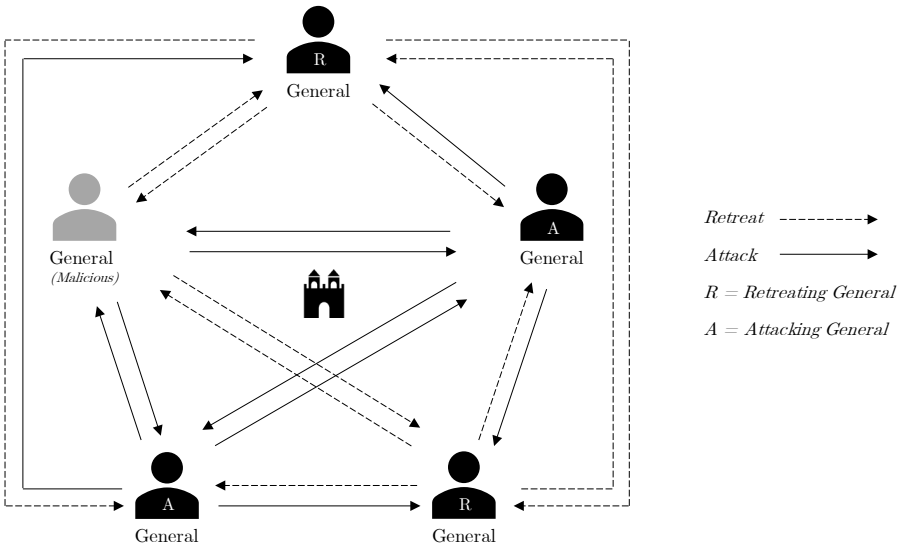

Figure 1: Byzantine General's Problem

Byzantine fault tolerance can be achieved if the non-malicious generals have a majority agreement on their strategy. Malicious generals may be present, but the system can remain Byzantine fault-tolerant as long as the number of malicious generals does not equal or exceed one third of all generals. It is not possible for an asynchronous system to provide both safety (the guarantee that all honest generals will eventually agree on what progress was made) and liveness (the ability to continue to make forward progress) with more than one third of the generals being malicious.

The proof for a solution to the Byzantine General's Problem can be likened to nodes on a decentralized, asynchronous network attempting to achieve consensus in the presence of suboptimal information. Suppose we have n nodes of which h are honest and d are dishonest ($n = h + d$). In the case where all honest nodes are evenly split on the two directions, the system could make forward progress. The malicious nodes could tell the honest nodes that they agree with them, such that $h/2 + d$ nodes agreeing on each of two conflicting ways the system could make forward progress. The honest nodes must not make forward progress, otherwise they will go in different directions and lose safety. Therefore, the number of nodes required to achieve this safety threshold must be greater than half the number of honest nodes plus the

number of malicious nodes. If we call t the threshold required to make forward progress, that gives us: $t > (h/2) + d$. This is the requirement for safety.

However, the malicious nodes could also fail to agree. Therefore, the number of nodes required to agree before we can make forward progress must be no more than the number of honest nodes or we lose liveness. This gives us $t <= h$ or $h >= t$. This is the condition for liveness. Combining the two results, we get:

$$\begin{gathered} h >= t > (h/2) + d \\ h > (h/2) + d \\ (h/2) > d \\ d < (h/2) \end{gathered}$$

As demonstrated, the number of faulty nodes we can tolerate is less than half the number of honest nodes. Therefore, we cannot tolerate 1/3 or more of the nodes being dishonest or we lose either safety or liveness. Byzantine Fault Tolerant systems requires both safety and liveness conditions to be met in order for the honest nodes to succeed.

4.2 Nakamoto Consensus, Native Currency & Double Spend

Satoshi Nakamoto proposed Bitcoin in 2008 as a peer-to-peer digital cash operated by a decentralized network. In order to align the interests of the curators of the ledger, transaction validators ("miners") are compensated using native money and are required to expend computational power in a "proof of work" scheme to solve the double spend problem.

The double spend problem is a potential flaw in a digital currency system in which the same single digital unit can be spent more than once. This is possible because a digital token consists of a digital file that can be duplicated or falsified. Since decentralized digital currencies have no central agency verifying that a unit is being spent only once, there is a risk that a unit can be spent more than once. Satoshi proposed a public, timestamped and log-based mechanism to generate computational proofs that would be able to verify the authenticity of each transaction and prevent double-spending.

To implement this mechanism, transactions are organized into timestamped blocks. The proof of work scheme involves computationally guessing for a value that when hashed (a mathematical mapping of an

arbitrary input to a unique output of fixed length) with the previous hashed block header, the hashed value is less than some adjustable number, referred to as the "difficulty." Once the computational effort and electricity has been expended to satisfy the proof of work, the block cannot be changed without redoing the work and blocks are chained together chronologically.

As subsequent blocks are attached to the chain, the work to change a block would require redoing the work calculations for all the blocks after it. The network can verify the work a miner has completed by executing a single hash. The system remains secure as long as the honest nodes collectively control more computational power than any cooperating group of attacker nodes. This is Satoshi's solution to the Byzantine General's Problem, otherwise known as the Nakamoto consensus.

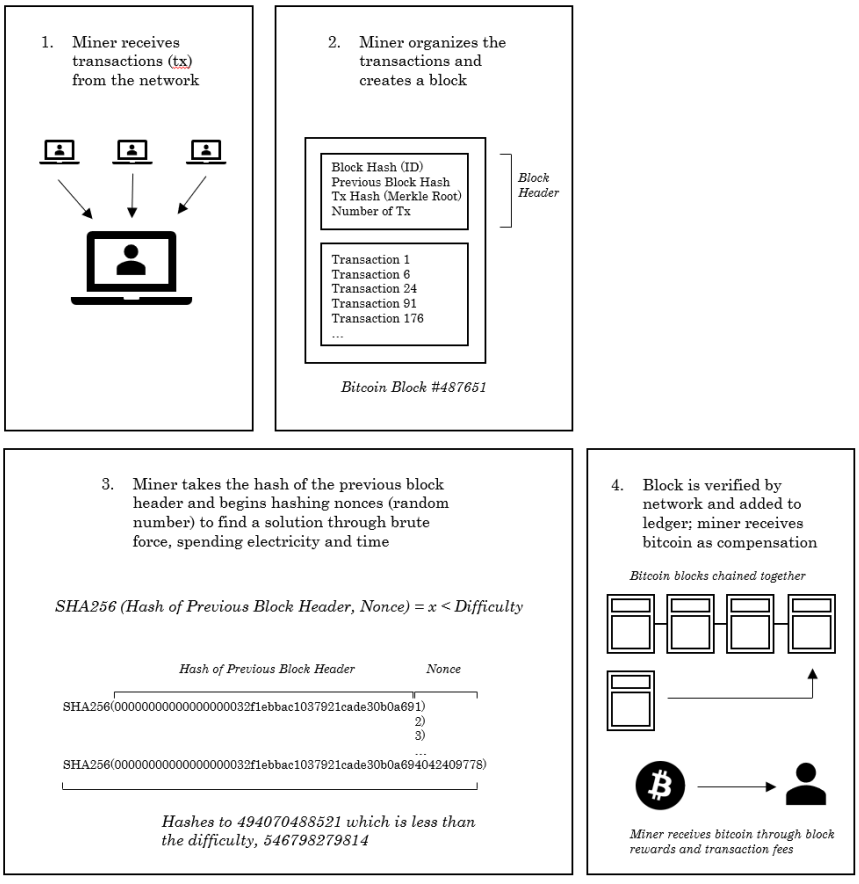

Figure 2: Bitcoin Mining Overview

Bitcoin solves the double spend problem by having a publicly-verifiable ledger. If an individual attempts to spend his or her bitcoin more than once, the miners will reject the invalid transaction. The ledger of transactions is updated with each new block, so that participants can calculate an individual's balance and verify whether they are attempting to double spend.

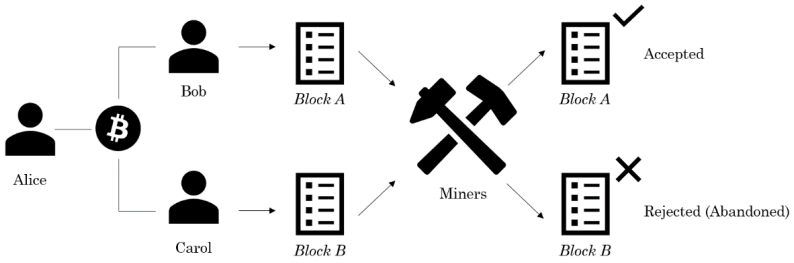

Figure 3: Double Spend Problem

In return for completing the verifiable work computation, the miners are compensated in bitcoin (the native currency) through block rewards and transaction fees. This native payment provides an incentive for miners to compute and verify the transactions chain. Furthermore, the expenditure of electricity and time creates an economic cost to miners that acts as a penalty if the miner is not acting honestly. If a miner attempts to cheat and broadcast a block with false information, the miner will not receive bitcoin and will incur the economic cost of mining. Costs include electricity, capital investments in specialized hardware, bandwidth, storage, and operational expenses. Compensation payments must be irreversible upon the network's consensus, natively digital and integrated, and operational 24/7 to support global transactions.

If external payment mechanisms were used, they would run into a variety of challenges. External payments depend on standard legal contracts and the rule of law, which requires an inefficient external party intervention in the event of a disagreement. External payments can be reversed, which creates an incentive to cheat miners, while native transactions cannot. External payments could be targeted and blocked by intermediaries, which would reduce the ability for the system to function under duress.

Through a dual incentive structure, miners on the Bitcoin network are incentivized to propagate the ledger of transactions and maintain the network while also solving the double spend and Byzantine General's Problem. Bitcoin was the first example of the described system, and it serves as a blueprint for much of the crypto-asset networks currently in operation.

4.3 Cryptographic Security & Digital Signatures

Practical Byzantine fault tolerance also requires unforgeable signatures to ensure that messages and transactions are authentic. Digital signatures in modern computer systems that use asymmetric or public-key cryptography can provide Byzantine fault tolerance, even in the presence of an arbitrary number of malicious actors. Public-key cryptography is a system that uses a pair of private and public keys. Public keys can be distributed widely, while private keys are known only to the owner.

Asymmetric cryptography achieves two functions. First, only the paired private key holder can decrypt the message encrypted with the public key. Second, the public key allows for the authentication and verification that a message was sent by the holder of the paired private key. The strength of a public key cryptography system is the computational effort required to find the private key from its paired public key. Effective security only requires keeping the private key confidential. The public key can be openly distributed without compromising security.

A digital signature is designed to verify that a message came from a particular sender, which prevents impersonation of the sender and denial by the sender of having sent the message. In practice, a message is signed using the sender's private signing key by encrypting the message with the private key. The digitally signed message is then sent to the recipient, who can then use the sender's public key to verify the signature by decrypting the message with the sender's public key. Through cryptographic security, the network can verify the authenticity of messages and transactions and ensure forward progress.

5 Conclusion

The critical alignment and incentivization of a global network of open-source programmers with the users provides an opportunity for innovation

and security of the Internet's infrastructure. Open and replicated databases limit the ability for centralized organizations to censor, delete, or abuse information. Advancements in cryptography allow networks to remain secure and protected. While digital ledgers and networks have existed for decades, the alignment through an economic incentive is a breakthrough in the creation, sharing, and governance of information networks. Private ledgers can still have disruptive business effects on trusted information management, but do not incentivize governance or innovation in open, trustless networks.

Open and secure decentralized networks coupled with incentivized governance represent an opportunity to change the way societies interact with one another. Satoshi's Bitcoin created a P2P money transfer system without a centralized party that incentivized participation and governance through a native currency. The creation and governance of the crypto asset networks of the last decade followed a similar blueprint that focused on various aspects of our Internet, ranging from digitally enforceable agreements through smart contracts, the representation, transfer, and consumption of digitally scare resources, and trustless applications. Increased financial and human capital investment in the development and maturation of decentralized technologies can disrupt the status quo and lead to a broader balance of decentralization and centralization in our digital infrastructure.