The Path to a Decentralized DNS, Overcoming Adoption Challenges, Domain Squatting, and “Group Trap” in Decentralized Systems

Agent86.BTS@gmail.com

8-2-2014

Introduction:

Domain name registry has become a controversial topic in recent times. The internet namespace is relied on by the public across the globe. Control over this critical infrastructure must be considered carefully. Events such as Edward Snowden's revelations about NSA spying have increased calls to move the domain name system out of the hands of ICANN and out of the control and jurisdiction of any single government. There is significant demand for a decentralized DNS managed in an incorruptible, transparent, and publically auditable manner. The current marketplace for domain ownership is also costly and inefficient. Domain squatting and domain sales remain sources of added cost and profiteering. Domain ownership disputes may be settled with costly litigation; a system not equally accessible to all market participants. The fair allocation of domains and avoidance of cybersquatting also presents a significant challenge to any replacement system. Despite demand, no new DNS system outside of ICANN has achieved broad use or adoption. In this paper a system is proposed to meet this market demand and overcome challenges to adoption.

Learning from the Past:

The concept of a decentralized DNS is not new. One prominent attempt is a project called "Namecoin." Namecoin is a DNS based heavily on the technology behind Bitcoin (1). Bitcoin introduced a novel method for a decentralized network to come to consensus on a shared ledger. A shared, publicly auditable ledger, beyond the control of any single institution or government, is a desirable system on which to implement a publically auditable DNS.

Despite creating such a transparent domain name registry, Namecoin has failed to gain traction with the public for a number of reasons. Firstly, Namecoin suffers from a lack of resources and economic incentives needed for growth and promotion. There is no mechanism to effectively direct sufficient resources to developers and promoters. Charitable donations toward these expenses are not sufficient. Secondly, a primary flaw in the Namecoin model is the lack of a system to address domain name squatting. While cybersquatting is a problem in our current system, there are some tools in place to address it. These tools include trademark disputes, litigation, and administrative actions. The problem of squatting is greatly amplified in systems that provide no feasible mechanism to address the issue. Finally, the consensus mechanism for the Namecoin ledger, adopted from Bitcoin, is not ideal and suffers from a tendency toward centralization over time.

Bitcoin demonstrated that a decentralized ledger can be used to track ownership rights. This concept has applications that go beyond tracking "coin" ownership as a form of money. Dan Larimer, who founded the BitShares project, made the observation that ownership stake tracked on a decentralized ledger is similar to "shares" of a decentralized company (2, 3). With this analogy in mind, we can more easily analyze the economic incentives for a decentralized system that provides a service. Typically, the ownership stake of the system acts as an internal currency for services provided and thus creates demand for shares. Payments to all shareholders are accomplished via destruction of shares such that each shareholder's percentage ownership is increased. In this case, the service provided is a domain name registry.

A DNS must be useful to website owners and the general public to be successfully adopted. Memorable domain names are a limited and valuable resource. Users expect a domain name system in which memorable domains have useful and appropriate content. Website owners want the ability to secure memorable and appropriate domain names at fair and competitive prices. Users and website owners both benefit from websites free from censorship, confiscation, and "man in the middle" attacks. Decentralized DNS models have an added market advantage of providing increased privacy to domain holders.

The BitShares analogy allows us to design a shareholder owned decentralized DNS service that provides for these market demands while financially rewarding shareholders for developing, maintaining and promoting the system. This system can be designed to solve the problems hindering Namecoin and other DNS alternatives.

Squatters:

The concept of domain name ownership should be explored carefully. The shareholders of a decentralized DNS may claim ultimate ownership interest of their namespace as they are burdened with maintaining it and promoting its widespread adoption. Shareholders are incentivized to maximize the utility and value of the namespace for all parties.

A simple system for domain name registration is a "first come first served" model with a fixed registration fee per domain and a nominal annual renewal fee. This is the model proposed by Namecoin. This model is grossly insufficient to prevent domain name squatting. When a system allows domain names to be purchased and held indefinitely at little cost it incentivizes early adopters to purchase large numbers of domain names with the hope of reselling some names at a profit to later adopters. This practice discourages real website developers from buying domains by driving up acquisition costs and creating a difficult, unpredictable, and frustrating purchasing process. These barriers ensure the system will never be broadly adopted or useful.

Rather than a simple "first come first served" model, it is possible to use an auction to initially award domains. This can also be followed by nominal renewal fees. While this may generate more value for shareholders, it does not solve the problem of squatting. Domains will still be bid on in mass for speculative value. This leaves the cost and aggravation for future buyers who must negotiate directly with domain squatters.

A recently proposed solution to domain name squatting has been documented within the BitShares community (4, 5). This system uses a modified initial auction format. The system rewards bidders who are outbid during an auction. The intention is to incentivize otherwise disinterested parties to bid up auction prices to ensure a "market rate" is reached. The author makes an unsupported assumption that speculators would bid above the long-term speculative value of the domain and that this will alter resale behavior as speculators are “incentivized to sell back bad bets at a loss” (4). There are also auction incentives that are hoped to encourage bidders to initially bid at the price they are willing to pay. This complex proposal offers very little improvement over a standard auction. The proposed system also does not address the root cause of squatting behavior which is the low cost to hold domains over time.

These deficiencies in addressing squatting behavior destroy the utility of all currently proposed decentralized DNS systems. Our current domain name system, while costly and inefficient, has tools to address squatting including litigation and administrative procedures. Without a system to address these challenges it is not plausible for an alternative DNS to compete for adoption. While it is conceivable that shareholders of a decentralized system could set up an analogous dispute resolution process such as voting on domain disputes, these processes tend to be costly, time consuming, and unpredictable.

Distribution of valuable and memorable domain names must be perceived as fair, broadly accessibly, transparent, and must promote utilization. A key to avoid abusive squatting is to make holding unused domains costly. Shareholders can retain ownership of the namespace while leasing domains at market determined prices. This tends to make it more profitable for speculators to hold shares of the DNS rather than squat domain names. Lease terms must be fair and respect the needs of website owners who are likely to make significant investments over time into their chosen domains.

Parameters:

The following system parameters are designed to maximize utility and fairness:

A new domain can be registered for an initial 30 day trial and used immediately. This is a benefit to users who want quick access to a domain. Doing so initiates a 30 day auction for a 1 year lease of the domain. The original auction initiator has access to the domain for the period of the auction.

Parameters for the initial auction should be fair, easy to understand, and reduce the need for complex bidding strategy.

Suggested auction parameters:

1) 30 day auction - ensures visibility of the auction so interested parties are unlikely to miss it.
2) Bids must be 10% above prior bid to be accepted - easy to remember and reduces back and forth.
3) Auction stays open after 30 days until there is 24 hours of inactivity - reduces desire to place a bid in the last minutes of the auction deadline. Auction is unlikely to remain open long after 30 days because the selling price would double at least every week (1.1^7 = 1.95).

After acquiring a lease, a domain holder may extend the lease at any time up to the max lease length. The max lease length is defined by the formula: initial_lease_length + time_domain_held = max_lease_length. Domains acquired from the auction process have an initial lease length of 1 year.

A domain name holder may post a sale offer for the remainder of their lease. They may set a price and an optional time delay to allow for transition. Selling at a price above their current lease rate sets a new higher market rate for the domain. Selling at a loss will not lower the future lease rate for the domain. The only way the shareholders will accept a lower lease rate on a domain is if the lease comes to the expiration date and a new 30 day auction is initiated. The current lessee may initiate a new auction within the last 30 days of their lease and also bid in the auction if they choose. They would retain control of the domain during the auction. Keep in mind, a lease should not get close to expiration unless it is over-priced as it can be extended at any time up to the max lease length.

Whether or not a domain is posted for sale, a party interested in acquiring a currently leased domain may place an upfront deposit on that domain at a rate at least 10% above the current lease rate for the full length of the current lease. At this point the current domain holder may:

1) Extend their lease at the higher market rate (this relinquishes the deposit back to the bidder)
2) Hold the lease until the expiration date. At this point the domain is relinquished to the higher bidder and the bidder takes over the lease with an initial term equal to the lease they bought out.
3) "Sub-lease" the domain to the higher bidder at any time before the lease expiration. Sub-leasing gives a profit to the original domain holder by the formula (higher_rate - rate_paid) * time_remaining_on_original_lease. The new holder always takes over the domain with a lease term equal to the length of the lease they bought out.

When bidding on a currently leased domain, the funds of the high bidder are tied up and only released back to them in the event the current holder extends their lease at the higher market rate or if the bidder is out-bid for the domain. The high bidder may acquire control of the domain for the full amount of their deposit either through a sublease or the current lease expiration.

There may be times when a high bidder gets "buyer's remorse" and would prefer to remove their offer to recover the deposit. An advanced option can allow a bidder in this situation to offer a "buyout incentive." This incentive is paid to anyone who takes action that releases them from their bid obligation. It is either paid to the current domain holder if they extend their lease at the higher market rate or it is paid to anyone who out-bids them for the domain.

Turning Squatters into Sales People:

The previously outlined parameters describe a system in which domains have a market based "carrying cost." Any individual who purchases a domain for the purpose of speculating on its future value must contend with this carrying cost. Speculators cannot afford to pay the same costs to carry a domain as someone with a legitimate use for the domain. Carrying costs motivate price speculators to promote names for a quicker sale; it turns squatters into sales people. An apt analogy is "house flipping" where carrying costs, such as property taxes, motivate the flipper to promote the home and sell quickly.

Carrying costs also make it prohibitively expensive to lease domains desired by competitors or adversaries in order to deny use of the domain. It is simply too expensive to maintain payments at high market rates for a multitude of unused domains.

Domain name holders who establish long term ownership interest in their domain are rewarded with very long lease options to have the certainty of future ownership. They are also rewarded with a much greater profit opportunity in the event a buyer is interested in the domain. As the system matures, long established leases may be available for purchase to those willing to pay the additional cost.

Group Trap:

A major barrier to adoption of a system such as Namecoin is the lack of resources and financial incentives for those who are promoting and developing the system. All current systems of decentralized ownership tracking, often grouped under the term "crypto-currencies" (which includes Bitcoin) suffer from a problem of "group trap." Essentially, these decentralized systems have no mechanism to effectively centralize resources to incentivize developers and promoters of the system. While those with stake in a particular currency have some motivation to promote it, the value of the work performed is diluted across all shareholders. A developer or promoter working hard for such a system personally incurs the cost of that labor while other shareholders do not. The shareholders who do not incur these extra costs derive comparatively better returns from their investment.

Many such systems begin with large stakeholders who work hard to promote and develop the system. As they begin to sell stake to cover costs it becomes apparent that the work is not adequately rewarded. Many of these projects leave investors holding stake in abandoned and underdeveloped projects. Some projects raise initial capital from investors who are then granted stake. This money is used on the honor system to develop the project. This starting capital is inherently limited, it is not controlled and directed by shareholders proportional to stake, and it is not a sustainable funding method for long term project costs.

The solution to this "group trap" is shareholder directed reinvestment or distribution. Following the BitShares analogy of shares in a profitable company we can see that shareholders can be given voting rights to direct capital. These systems can be structured in a way that generates profit for shareholders. For instance, a domain holder can pay a certain amount of stake to the network to lease a domain. This stake is destroyed, increasing the percent ownership of all stakeholders. The stakeholders can then sell that additional stake back to customers who use it to pay to lease domains on the network and the stake is again destroyed. Destroyed stake is essentially "income" to the shareholders. While destroyed shares are income, shareholders can pay expenses via creation of new shares.

A method to accomplish this is the election by popular vote of "workers" who are paid via the issuance of new shares. Workers can be elected by a method called "approval voting." Approval voting allows any stakeholder to approve or not approve of any candidate worker. These approvals are weighted by ownership stake. Workers with over 50% approval by stake become active and are paid a salary in newly issued shares. This salary could be specified by the worker as part of their candidacy. It is also possible to allow shareholders additional control of salary by approving a percentage of the requested salary during voting. This percentage could be above or below the requested salary and a median can be taken to determine the actual paid salary. This system allows shareholders to hire executives, developers, and promoters and appropriately incentivize them to work in the interests of the system.

A domain registration system is the type of system that requires a large network effect. Utility of the system and adoption of the system are interdependent and each is reinforced by the other. Promoting the system to the point that a network effect is established may require a large initial investment. It is quite likely that expenses for development and promotion would outweigh income in the early stages of the system. For this reason the system may create more shares than it destroys in early stages. The system would grow in value by increasing adoption and attracting new investment capital to buy the newly created shares.

Consensus:

A final barrier to the long term success of Namecoin is the choice of consensus algorithm. A detailed technical discussion of consensus algorithms is beyond the scope of this paper; however a useful overview can be given.

Namecoin uses a "proof of work" algorithm whereby adding a block of transactions to the shared ledger requires a solution to a difficult and computationally intensive problem. This mathematical problem is difficult to solve but easy to check. The network builds off and forms consensus on the ledger that represents the most verified "computational work." The idea is that in order to control the ledger an entity must perform more computational work than the rest of the network combined. This work is rewarded with the issuance of new shares or "coins." Although Namecoin is secured via the same work and computers that secure the Bitcoin network (it does not require significant additional resources) this type of competitive computation inevitably leads to centralization. Motivated by profit, specialized hardware is developed to reduce costs. Due to economies of scale, only the largest and most efficient operations can profitably participate. The computational energy required for proof of work is also unnecessarily wasteful when compared to other options for consensus.

A much improved algorithm for consensus is "proof of stake." A specific form of proof of stake called "delegated proof of stake" (DPOS) has advantages over other implementations (6). DPOS allows the election of representatives called “delegates” to validate transactions on the network. This work is verifiable, and if not performed, delegates are removed. Proof of stake rests power over the ledger ultimately in the hands of those with ownership stake. Proof of work gives power over the ledger to those with access to the most computational resources. Delegated proof of stake allows a more sustainable, cost efficient, and secure shared ledger than proof of work can provide.

Conclusion:

This paper has outlined a structure for a decentralized DNS which may overcome current barriers and create the right incentives for broad adoption. A sustainable funding and economic incentive model has been proposed. Market parameters have been outlined that promote utility and fairness and discourage domain squatting. A decentralized DNS can provide transparency and accessibility. It can reduce costs and reduce the opportunity for any single entity or government to exercise control over the public DNS system.

References:

1) Double, Chris. May 2011. “Namecoin - A DNS alternative based on Bitcoin.” http://bluishcoder.co.nz/2011/05/12/namecoin-a-dns-alternative-based-on-bitcoin.html

2) Larimer, Stan. September 2013. “Bitcoin & the Three Laws of Robotics.” http://bitshares.org/bitcoin-the-three-laws-of-robotics/

3) Larimer, Dan. November 2013. “Dac Revisited.” http://bitshares.org/dac-revisited/

4) Mushegian, Nikolai, June 2014. “DNS .p2p Auction Specification.” https://github.com/BitShares/bitshares_toolkit/wiki/DNS-.p2p-Auction-Specification

5) Mushegian, Nikolai, April 2014. “Whitepaper Draft.” https://github.com/nmushegian/dns/blob/master/whitepaper-draft.md

6) Larimer, Dan. April 2014. “Delegated Proof of Stake.” http://bitshares.org/delegated-proof-of-stake/