DOT-BIP WHITEPAPER

a/k/a Proposal for Implementing Dot-Bip decentralized DNS to create distributed, difficult-to-censor DNS-type function over the BipCoin cryptocurrency blockchain while solving all the problems that kept Namecoin from becoming adopted as anything other than a speculative commodity

SUMMARY:

We are going to make something that is so difficult to censor, someone could use it to say horrible, untrue things about *us* and there's no way that even *we* could take it down.

We believe this is the truest definition of actual free speech.

Several systems have attempted to do this. The one that came closest was Namecoin. But Namecoin was never used by more than a couple dozen websites for censor-proof DNS.

We plan to create something that will get wide scale adoption. That's the key to truly keeping speech free.

Dot-Bit Whitepaper v1.0
11/25/2016

Whitepaper written by the BipDevs (BipCoin dev team.)
bipcoin@gmail.com
https://bipcoin.org/

Dot-Bip DNS via BipCoin WILL BE BETTER than Dot-Bit via NameCoin BECAUSE:

--Dot-Bip SOLVES THE DOMAIN SQUATTING ISSUE

--Dot-Bip has an easy to use domain resolver issued on day one of Dot-Bip

--Domain resolver for Dot-Bip is SYSTEM WIDE

--Domain resolver Dot-Bip is easy to use for everyone

--Dot-Bip resolver is built into GUI wallet.

--Resolver won't go stale with third-party API updates.

--Coins are NOT destroyed when registering a domain

--Light clients will be very easy to build and update

--People will be encouraged to add third-party services

--Dot-Bip will pre-solve the security issue that was discovered in Namecoin

--No mission bloat

OVERVIEW:
We the BipDevs (BipCoin dev team) have great respect for the mission of Namecoin.

Namecoin was the *first* altcoin, and had a great idea: removing DNS registration and maintenance from the control of governments that can change at a whim (or with the election of a new "leader") and outlaw many types of free speech.

Namecoin has seen a lot of mining, trading and speculation. But it has never had much adoption for its intended purpose: circumventing censorship.

We have seen a lot of domain censorship around the world since the release of Namecoin in the spring of 2011. But Namecoin has never been used for to keep websites viewable in a country where censorship occurs. Sure, Namecoin devs might be able to point to one or two examples with three or four users, but that's really not "DNS-like" to speak of. To

have any value, and to have people develop services, and for webmasters and web users to want to use it, a DNS-like system has to have at least *somewhat* wide adoption.

Also, one of Namecoin's many problems was cybersquatting. Any name you wanted was probably already taken within months of the release of Namecoin.

In 2014, two people who are now BipDevs created MeowBit. MeowBit is a domain resolver for Namecoin Dot-Bit domains that improved on FreeSpeechMe, the domain resolver for Namecoin developed by a Namecoin dev team member.

These future BipDevs who made MeowBit had dealings with members of the Namecoin Dev team, plus studied their work and words a lot. The BipDevs have also studied the distributed DNS problem extensively.

The BipDevs now know what to do, and what *not* to do, in order to make distributed DNS work, and gain widespread adoption.

-=-=-=-=-=-=-=-=-

WHAT IS DISTRIBUTED DNS?

First, if you have never used Namecoin, let me briefly explain how domain registration works in that, since our mechanism in BipCoin for domain registration will be similar in some ways. (But not others.)

Unlike with standard domain registrars, with Namecoin, you do NOT send a payment to a company that does the registration and keeps it in their records that go into the (censorable) ICANN records.....Those records behind the scenes let everyone's browsers turn human-readable domain addresses (like **BipCoin.org**) into underlying IP addresses that computers can process. (Like **167.114.13.200**).

In Namecoin, it happens automatically and happens on the blockchain. It does not involve some company doing something for you.

Users do a process from within the CLI or GUI wallet, it costs them some coin, and the daemon adds the registration pair (domain name:IP address) into a block of the block chain, just like a transaction record.

Their top-level domain, .bit, is not accessible from normal browsers without special add-on software.

Users who have that software, plus the Namecoin blockchain on their local machine, or a light client that points to the blockchain elsewhere, can resolve Namecoin Dot-Bit addresses into actual web addresses.

These address are harder to censor than normal .com, .org, .eu (etc) addresses, Those domains can be taken down by government agencies demanding that the domain registrar essentially un-register the domain.

With Namecoin, if the IP of the server changes later, webmasters can make an update easily with another transaction from within the wallet. Domains can also be transferred to another owner (Namecoin address) from within the wallet.

All this is as secure as sending a Bitcoin transaction, and much harder to censor.

All of this will work the essentially the same in BipCoin, but this is where the similarity ends.

=-=-=--=-=-=

> NOTE: It is not technically correct to call our system or the Namecoin system "Distributed DNS" or "Blockchain DNS." This is because "DNS" is a proper noun. i.e. it describes an actual system, not a type of system. DNS is the current Domain Name System intertwined with the government-backed ICANN.
>
> But the phrase "DNS" has largely been made generic, so it's not uncommon to hear people call any DNS-like system "DNS."
>
> So, throughout this whitepaper we do call our system "DNS" for brevity....And to avoid having long stupid awkward sentence constructions over and over.
>
> A great shorthand name for our system is "Dot-Bip", since that will be the domain extension. (Named after "BipCoin", and Namecoin uses "Dot-Bit" for their extension). "Dot-Bit" sounded cool, but too geeky for the public. "Dot-Bip", sounds geeky, but also fun and not intimidating.

-=-=-=-=-=-=-=-

(Longer form):
Dot-Bip DNS via BipCoin will be BETTER than Dot-Bit via NameCoin BECAUSE:

--**Dot-Bip SOLVES DOMAIN SQUATTING ISSUE**. Dot-Bit domains via Namecoin only cost about 8 Euro cents for much of Namecoin's existence. At the beginning and later it was much cheaper. Every noun in the English language was registered Dot-Bit within a few months of the release of Namecoin. This made it virtually impossible for people to get the domain they want.

Dot-Bip addresses for a domain or ID via BipCoin will cost 8 dollars US (Mid-Nov 2016) of BipCoin for approximately one year, or 200 US dollars of BipCoin forever. This is reasonable (and cheaper than Dot-Com and other government-controlled domain registrations, but not so cheap as to encourage squatting).

--**Dot-Bip has an easy to use domain resolver issued on day one of Dot-Bip**, not 3 years later like the Dot-Bit resolver of Namecoin. (Namecoin's resolver was called FreeSpeechMe, which was named by a current BipCoin developer.)

--**Domain resolver MeowBip for Dot-Bip is SYSTEM WIDE**, not for one browser only as with FreeSpeechMe Namecoin. Namecoin's FreeSpeechMe only worked on www, and only via Firefox. BipCoin's MeowBit resolver will make ANYTHING on your computer resolve a Dot-Bip address. That includes all browsers, e-mail, FTP, IRC, Pidgin, etc.

--Domain resolver Dot-Bip is easy to use for everyone, and run in the background, invisibly. FreeSpeechMe

Namecoin's resolver, FreeSpeechMe, was not easy use by non-technical people, and it crashed. And the *horrible* Namecoin wallet that had to be running also *took ten minutes to open* before it would begin syncing. This turned off all but the most dedicated and stubborn "I ***WILL*** GET THIS TO WORK" users.

--**Resolver won't go stale with third-party API updates**. Namecoin's resolver, FreeSpeechMe, stopped working mid-2016 due to a Firefox update, and their dev team hasn't gotten around to updating it.

--**Dot-Bip resolver, MeowBip, is built into BipCoin the GUI wallet**. Namecoin dev team's official resolver, FreeSpeechMe, was a plug-in for Firefox only.

--Coins are NOT destroyed when registering a domain or ID or anything (unlike with Namecoin).

--**Light clients will be very easy to build and update**, using lists of nodes which will be easy to create and maintain via "tasting" the network.

Could also be done if we release software like this:
https://bit.no.com/
and then make it easy for people to run as part of BipCoin node.

--**People will be encouraged to add third-party services for Dot-Bip**. Unlike the Namecoin team, who got upset when OneName started doing ID and BTC address shortening over Namecoin:
https://www.reddit.com/r/Namecoin/comments/200tfs/onename_decentralized_identity_system_built_on/cfyzqvy/

Namecoin devs were mad at OneName for working on something without checking with Namecoin devs first. lol.

OneName moved their project over to the Bitcoin blockchain, and has use there today.

--**Dot-Bip will pre-solve the huge security issue that was discovered and fixed in Namecoin 2 years after launch**
http://www.coindesk.com/namecoin-flaw-patch-needed/

https://www.reddit.com/r/Bitcoin/comments/1ohyom/fatal_flaw_in_namecoin_found_doesnt_enforce_some/

--**No mission bloat**. BipCoin devs "see the forest for the trees." The Namecoin team was still working on many extended features before having any way for the general public to view a Dot-Bit domain. And this was while they still had a wallet that took more than 10 minutes to even open. And that's before it even *starts* updating the blockchain.

BipCoin Dot-Bip domain registration, and resolving of domains, is built into our GUI wallet. And it is easy to register, transfer and resolve domains for people who do not have a lot of technical understanding. We also have made extensive, easy to use tutorials on all features.

Any functions added later will be easy to use on day of release for people who do not have a lot of technical understanding.

There are some blockchain-based systems that say in theory that they may be able to provide distributed DNS; Maidsafe, EtherID via Ethereum, and some convoluted plan that once was in the works for Bitshares. That one kept changing what it did and how it worked. Not surprisingly, it collapsed.

But *none* of these, working or theoretical, deal well with the domain squatting problem. And some tried to deal with it by making people *bid* on domains, which drive the price them out of the reach of most people.

And some of them (particularly the now-dead Bitshares DNS) were / are too difficult to explain to non-technical people. Not the underlying core, but even how to register a domain. That is NOT a step toward adoption.

None of these DNS solutions have much/any adoption. **Adoption is the key**. Without adoption, any service that claims to offer this is just theories put forth by theorists.

And that includes Namecoin.

Some would jump in here and say "Steemit sort of does provide something like this" (including actual HOSTING of text-only material on their giant corporate blockchain).

But Steemit doesn't even *approach* actual decentralized. Because the founders can and do vastly drive up the visibility of some posts. Worse by far, they can *censor* anything they want. So in effect, the Steem board become the government in that system.

Many current blockchain systems go far beyond Namecoin in complexity, particularly in Decentralized Autonomous Organizations. But we believe the Namecoin idea had its simple merits. And we believe the huge problems of Namecoin can be fixed by using what basically amounts to some tiny bonehead-simple DAO-type things, while avoiding problems of complex exploitability like with *THE* DAO.

(Also, all those hugely popular centralized corporate blockchains that are supposed to make everything decentralized, have any of them done it? Do you know any people who are using any alternative DNS system, either as a webmaster or as a web viewer? There may be a few geeks reading this who know one or two people doing that, but that is not adoption. We believe we can make this easy enough to use and at a reasonable registration price to *actually get* wide adoption.

Corporate blockchains can be censored from outside too. Because there isn't a corporation anywhere that wouldn't at least consider responding to a cease and desist threat.

We're not making some hippie case for "corporations are bad, um'kay"? We're making the case that corporations are a horrible choice to oversee something where the goal is uncensorable DNS (or uncensorable *anything*).

Corporations also have a legal obligation to make any decisions they have to (within the law) to make a profit. So if a government organization wanted to partner with some blockchain corporation and it was more profitable to partner with a government than with a private org, the corporate officers could go to *jail* for refusing that partnership on moral grounds. And governments can always outbid the private sector because governments can steal, print and inflate money as much as they'd like.

Here's what we're looking to make. Something that is so difficult to censor, that someone could use it to say horrible untrue things about the BipDevs and there's no way that we could take it down.

We believe that is the truest definition of actual free speech, and it's what the Internet was SUPPOSED to be, but never yet really has been.

I mean, there is TOR, which makes sites hard to censor because it's hard to find where they're hosted. But, but TOR is hard to use for webmaster and user to use. And even harder to use correctly. (There is a theory that Ross Unbricht is in jail because of problems with a particular version of TOR or intentional backdoors in all versions of TOR. And most people don't know this, but TOR is still to this day funded by a government agency:
https://en.wikipedia.org/wiki/Tor_(anonymity_network)#History

With the incoming regime in the US, this will become very important very soon.
Not that it would have been much better under Hilary, she is practically owned by bankers and used dirty tactics to silence critics of her.
http://www.judicialwatch.org/blog/2015/11/clinton-goes-after-laugh-factory-comedians-for-making-fun-of-her/

They're all horrible. All politicians, in every nation, throughout history, past present and future, all want to take your freedom of speech and freedom of everything. Any differences are just a matter of movable points on a continuum.

-=-=-=-=-=-=-=-=-=

MECHANISM FOR PREVENTING DOMAIN SQUATTING:
Domain squatting was a *gigantic* issue for Namecoin., though Namecoin devs were totally in denial about this:[1]

Namecoin core dev domob1812 called domain squatting on Dot-Bit "a small problem" (!), even after Namecoin had been out for 3 years and almost all common English words, and many company names, were squatted. (It's item #2 in his post here):
https://www.reddit.com/r/Namecoin/comments/200tfs/onename_decentralized_identity_system_built_on/cfyzqvy/

Not only were almost all available names squatted on Namecoin, there was/is no way to purchase those squatted domains if you wanted to bite your pride and pay a lot for one. None of the domains have the typical "email us if you want to buy this domain" placeholder page that is common with squatted Dot-Com domains. So there is no way to find out a way to pay someone for a squatted Namecoin domain!

WHAT IF SOMEONE DOES GET THE DOMAIN I WANT?
Well, there will certainly be no domain dispute resolution. If someone gets
(YourCompanyName).bip,
then you register
(YourCompanyNameDroneProof).bip

[1] It may seem that the BipCoin dev writing this whitepaper have it out to bash Namecoin and the Namecoin devs. It's not personal. It's this: there is *no possible way* to accurately explain what was wrong with Namecoin (and what to do *right* in moving distributed DNS *beyond* Namecoin) without mentioning the mistakes of the Namecoin devs.

For what it's worth, the Namecoin devs are brilliant guys, but seem to lack common sense. Sort of the way it is said that Albert Einstein would walk out in the snow and forget his shoes. The Namecoin guys are brilliant math geeks, but really didn't know what to do with the great beginning they had.

They were often their own worst enemies as far as working toward actual adoption.

It almost seems like they didn't really *want* adoption, because that would involve dealing with actual humans. Most of that team seem much happier programming than interacting with others.

Or
(RealYourCompanyName).bip

(Domains are not case-sensitive, but that's the idea.) Also, if the name isn't registered for all time, you could watch for when it expires and grab it then.

A few common things will likely be squatted anyway, like
Art.bip
Computer.bip
Sex.bip
Drugs.bip

But that exists in any domain system. Plus a little bit of that is good for the economy of a system. And domains won't be so cheap that anyone is going to register every word.

And you could always get
DebbiesArt.bip
MyComputer.bip
BestSex.bip
etc.

It is our opinion that too much emphasis was based on the value of actual domains in the past, during the Dot-Com gold rush in the late 90s especially. It was an unknown new world, and there really wasn't a way to apply true market valuations on domains back then.

The thing you really want to do is get a domain that defines you or your business, is easy to remember, and cannot be taken down, which is what Dot-Bip does.

BUT WHAT IF MY IP CHANGES?
You can update that very easily for a tiny amount of BipCoin, and changes will be seen throughout the network far faster than when you update a Dot-Com IP.

WHAT IF SOMEONE TRIES TO HIJACK THE .BIP TOP LEVEL DOMAIN?
If someone made a competing system, or a system just to mess with Dot-Bip, and made their system also use the Dot-Bip system, domains registered with their system would not resolve on our system, because they would not be in our blockchain.

Anyone else could use the pricing and adoption mechanism we created and make a different top-level domain on a different blockchain. But we'd probably still win the war of adoption.

We have people on our team, including one of the non-programmersdriving everything, that they don't have. Ideas cannot be "stolen", especially if they involve *you* as an integral part of the equation.

SO HOW WILL Dot-Bit DETERMINE COST OF REGISTERING A DOMAIN?
We will be hard-code pegging the price in BipCoin **to the price in gold.**

This has been suggested before, but has never been implemented in a way that had any adoption at all for DNS. And even outside of DNS, it hasn't really made it out of the theoretical stage.

There have been attempts to peg the price of a cryptocurrency itself to gold, but *that's not how this works*. Devs don't get to say "our coins is worth X." That is the job of the market.

The daemon will average BipCoin of all exchanges accessible at that moment that currently take BipCoin and can display the price in dollars or euros. So registering a Dot-Bip domain for one year is always 8 dollars US worth of BipCoin at time of this writing (mid-November, 2016).

That's a little cheaper than a lot of Dot-Com domain registrars per year, but high enough that it will *heavily* discourage squatting.

We're pegging to gold, not dollars or euros, due to regime uncertainty after recent USA election.

Gold is also just a better stable commodity price in general. The amount of labor in a given job type has been payable in about the same amount of gold for hundreds, and sometimes thousands, of years.

Free APIs for gold price are not terribly common, many charge, but we can find some. Gold is stable enough that even using 30-day average and the daemon only checking once every 30 days for a 30-day average would be fine. Or maybe every 15 days for a 15-day average. BipCoin would be checked every eight hours.

If the network can't contact any of the current BipCoin or gold exchanges, it will go with the last good price and check again for gold price in a day and BipCoin price in an hour.

It may be easier to find free gold price APIs that serve a gold price that's a few days stale, than a current price. A few days stale would likely work fine, at least for proof of concept.

The price of gold is stable(ish) enough that the idea is really just to get a price that’s not wildly off. Like let’s say accurate to within 35% either way of current price.

> **Registering a Dot-Bip domain for about one year (478,800 blocks) should cost the same as *200 mg of .999 pure gold's worth of BipCoin.***

(This is about 8 dollars US from the 30-day average gold price at the time of this writing.)

Registering a Dot-Bip domain for all time should cost the same as *5 grams of 999 pure gold's worth of BipCoin.*
(This is about 200 dollars US from the 30-day average gold price at the time of this writing.)

The price of an approximate one-year domain registration **will be half this price for first approximate one-year** (478,800 blocks) to encourage adoption. And during this period the "for all time" domain registration price will be 2/3.

NOTE: If registering or updating domains is ever temporarily unavailable for some reason, Dot-Bip via BipCoin will still allow *viewing* any previously registered domains.

DISCOURAGING CRACKING
We store the domain registration price in the blockchain, so someone can't alter our code, compile the result, and register domains cheaper than anyone else. It works like this:

The price goes in the blocks. If the nodes can't verify the price is valid, the block is not accepted.

When a user registers a domain, it must be done using the price of gold as recorded in the last block. When a block is built, part of the validation done by the nodes that accept the block is that the price of gold recorded in that block can be verified. Otherwise, the block is rejected, just like a block would be rejected if it had other problems. The pricing is in the blocks and is part of the validation.

An interesting byproduct is that in the process of doing this, we're also storing the historical price of gold in the blockchain.

BipCoin Dot-Bip checks THE network each time you register or update a domain, but only checks BipCoin exchanges one time every eight hours for whole network, so we don't overwhelm exchanges with too much traffic. But it would be good our network has more than one IP to check for each exchange.

With the system to check with the historical price of gold to make sure no one is compiling the code and cheating it to mass-register many domains....The problem is that while gold is generally stable, it has had some HUGE dips and rises, especially with problems with the US Dollar or the Euro or whatever currency you compare it to.

Historical gold price data here: http://www.kitco.com/charts/historicalgold.html

The nodes go check the gold price and it has to be within 20% of what they see in order for the block to be accepted. To hack that they would have to change all the other nodes code, not just their miner's code.

*The **miners** are never trusted, they are only verified.*

WHAT IF GOLD BECOMES INCREDIBLY CHEAP?
That's unlikely, but let's say someone *does* achieve the alchemist's dream of turning lead to gold….without an incredibly expensive-to-run particle accelerator.

More likely it would actually be finding a cheap way of extracting gold from seawater. But let's say gold plummets to the price of steel. (71 USD per ton at the time of this writing.) Well, Dot-Bip would still work after a quick software update.

Even if the original team is gone, anyone could make the update. Then as long as it were on public repositories (including Dot-Bit ones if this all became illegal), reviewed by people, then compiled from those repositories to avoid backdoors…..As long as the new software were adopted by most miners and nodes, it would work.

And people *would* update quickly. Because anyone invested in having this system work would scramble to keep it working. It's unlikely that there would even be a discussion.

So as soon as a software update was issued, very inexpensive gold would STILL work as the price reference for Dot-Bip, as long as that low price stayed relatively stable, and were adjusted to the original actual prices at the time of this writing.

WHAT IF THE PRICE OF GOLD DOES *NOT* STAY STABLE?
Let's say some newly elected billionaire president of a nation with a major economy doesn't like common serfs owning gold, because he want to maintain even more control on the currency to keep his rich buddies rich and everyone else scrambling to survive. So he outlaws ownership of gold, thus making gold black market and having wide price fluctuations?

If the price of gold does not stay stable, the wallet software could be updated to pin to *any* somewhat stable commodity: silver, platinum, pork bellies, soy, steel, lumber, wheat, legal marijuana, etc.

A price fluctuation of even 50% up or down over a long time line is even ok. First because these things usually correct themselves. Second, half price or double price of registering a domain is fine. It's wild price fluctuations of like Namecoin had that we are avoiding with this system. Namecoin made it a set amount of coin to register a domain. The price has varied 4500% from lowest to most expensive, and is back down near its lowest now.

So registering a Namecoin domain started so cheap that someone squatted every English word as a domain, to so expensive most people wouldn't register a domain, and back down to where even uncommon word combinations are now being squatted.

So basically the price of registering a Namecoin domain has historically had a hyperinflation rate approaching that of 1923 Germany's Weimar Republic, where people were burning the paper money to keep warm, and the price of a meal in a restaurant would go up vastly in the time it took to eat the meal.

Pegging the BipCoin cost of registration to almost *any* commonly traded real-world commodity would work. **Because none of them have 4500% price swings like Namecoin.**

WHY BipCoin? WHY NOT MAKE A NEW COIN TO DO THIS?
BipCoin exists. It's trade and mined. It's new enough to not be too difficult to mine, but not so hard to mine that people don't mine it. Thus, it works very well.

Put it this way: BipCoin transactions confirm faster than with Bitcoin 100% of the time. Sure, this is partly from shorter block time but it's also partly from far less traffic and enough mining to make it *work*. A new coin would not be guaranteed to have that.

And BipCoin has never had some huge spilt that lost people millions of dollars and divided communities.

BipCoin is also a known thing. It's traded. It's on an exchange. It's on price calculator websites. It's on market cap websites. CLI and GUI wallets exist already for Windows and Linux. There are extraordinarily detailed tech documentation on the BipCoin website that make it easy to use for noobs. In fact, a lot of people mining BipCoin never mined anything before, and some *never even transacted with Bitcoin* before.
So, there is a small but very committed community already backing BipCoin.

A new coin would have to start all this from scratch.

Also, unlike Bitcoin, BipCoin uses CryptoNote code, which makes transactions truly anonymous, unlike Bitcoin and also unlike most altcoins.

ROAD MAP FOR IMPROVEMENTS
Our proof-of-concept release could start with one crypto exchange and one gold price source. Eventually we'd want many more, to average from, and for redundancy / decentralization.

But one of each will work for first proof-of-concept Dot-Bip BipCoin software release. (BipCoin is only on one exchange at the time of this writing. But more will surely be added as this takes off.)

Gold is likely to remain far less volatile than the euro, the dollar or any government currency, or than Bitcoin. Though the conversion in the daemon would take place from the gold price in dollars or euros to the current price of BipCoin in dollars or euros.

If we're getting gold prices in ounces, remember that gold is measured in *troy* ounces (approximately 31.1 grams) not in *avoirdupois* ounces (commonly called "ounces", which are used for most things except metals). An avoirdupois ounce is equal to approximately 28.3 grams).

8 dollars US is cheap enough to be reasonable, but expensive enough to discourage squatting. It was six cents worth of Namecoin to register a domain at the *peak* price of Namecoin, and much cheaper at both ends of its lifecycle. This is why before most people had heard of Namecoin, someone registered every word in the English dictionary as a Dot-Bit domain. lol.

Also, 8 dollars of BipCoin to register for 478,800 blocks (about one year), but 200 dollars of BipCoin to register forever. 200 dollars may seem high, but will also encourage people to become whales in BipCoin.

This may also encourage people to watch BipCoin closely to find the right moment to register. People might develop services to try to find the perfect moment to register. (Based on fluctuating prices of BipCoin, not of gold.)

But 8 dollars of BipCoin for one year is low enough that anyone who can afford a cheap web host can afford to register a Dot-Bip address. So no one is excluded.

The obvious and easy way to do all this would be to have the price update from a call to our website. But that is not acceptable because it's not decentralized. We to have it the BipCoin daemon itself do the work. We need to have it work even if the devs were taken out of the picture. And it could still work, because miners could decide which exchanges to add to the gold list and the BipCoin list, and miners would accept if it was adopted by adopting the updated software.

The software is on GitHub, but subsequent releases with source code will also be released as torrents so even if the source were removed from Git, the project could continue.

There are points of failure, in the exchanges where the updated price of BipCoin and the price of gold is taken from. But more would be added in updates as more exchanges start adding BipCoin. Eventually there would be enough for this mechanism to pass beyond being described as "distributed" and really start being definable as "decentralized."

If Dot-Bip catches on, some exchanges might start incorporating the price of gold to BipCoin in their API, saving the trouble of pinging both precious metal exchanges and cryptocurrency exchanges.

BUT IS THAT REALLY *DECENTRALIZED*?
The first version proof-of-concept will not be. As we add more exchanges for both BipCoin and for gold price, it will approach decentralization.

The difference between something being *distributed* and being *decentralized* is largely a mater of quantity. They're not really two discrete things, they're actually two regions of dots on a continuum.

Having the daemon check one exchange each for BipCoin and gold is barely even "distributed." Having the daemon check 100 exchanges each for BipCoin and gold would meet most, if not all, definitions of "decentralized."

Something in the middle, maybe even as low as five or ten exchanges each, would be harder to censor than an ICANN-controlled domain, for sure.
Most things called "decentralized" are actually just "distributed" on a large scale. This includes Bitcoin, where a board makes decisions on changes. This board, a small group of people, fighting changing block size, is part of what lead to the creation of Zcash by others.

All it takes to create a new disruptive system is a resentment and a coffee pot. lol.

The Bitcoin Foundation board decides on some changes. And whether they are implemented is determined by adoption which mining software is accepted by the larger mining pools.

What this really amounts to is that *under a dozen people control decisions* of what is and isn't adopted in "decentralized" Bitcoin.

We're really concerned less if Dot-Bit meets the absolute most extreme academic definition of "decentralized", and more concerned that it meets these criteria:

--It should be much harder to censor than an ICANN-controlled domain.

--It should satisfy Zooko's Triangle

--It should encourage and receive large-scale adoption. Not just BipCoin as a commodity of exchange, but the use of Dot-Bit for domain registrations, with many people possessing the ability to view them, even if just as emergency backups waiting in the wings for when domain names are seized.

--It can survive all members of the team being removed from the project, and be maintained by volunteers who never even had contact with the first team.

We believe Dot-Bit can meet these requirements 100% within 3 years of release.

(There are no plans for the team to leave, we just want the software to be able to function perfectly without us, like Bitcoin functions without Satoshi.)

If something happened to the core team before then, anyone else could take over the software production using code on GitHub (and on torrents), and as long as their software was accepted by the miners, the project could continue.

A precious metals dealership has graciously allowed us to use their API for gold price for the initial roll out.

MECHANISM FOR CHECKING BipCoin PRICE

We add a random number generator in daemon that would determine a period in the 4-hour window for every instance of software to check the exchange(s) for the current price of BipCoin (in dollars or euros) to gold (in dollars or euros).

Once the first 5 daemon instances have returned a price, they are automatically averaged, and that becomes the price for that four-hour period.

Then all other daemon instances on the network are told to NOT check (if their time hasn't come up yet. Random number generator would keep all wallets from checking at once and overwhelming the exchange(s).

Once the price for that period has been determined, there's a flag put in a block that tells the network "This is the price of registering a domain for next 120 blocks, and no other daemon instances should check the price during this 120 block period."

This could be broadcast to the network via Derrick's Blockchain Notification System. This is something that he made previously for Dot-Bit via Namecoin. For that we only used it to signal wallet owners when there was an update to install.

(Four-hour time is approx. Actually would happen every 120 blocks)

RENEWAL OF REGISTRATIONS

Unlike ICANN-controlled domains through domain registrars, you will NOT receive an automatic email when it's time to renew your domain, but services that provide this for a small amount of bips will be created by third parties. This will be especially important, since the registration period, 478,800 blocks, is not exactly one year, and can vary depending on the falling and rising of the hash rate of the BipCoin network.

-=-=-=-=-=-=-

FUNCTIONS THAT WILL BE POSSIBLE UPON RELEASE:
--Domain registration

-- Derrick's Blockchain Notification System**, the feature that Derrick added for Notification from Dev to users**, alerts via blockchain. (Could be used for mechanism to broadcast price of BipCoin to network.)

http://www.meowbit.com/meowbit-now-with-update-alerts-over-the-blockchain-a-new-feature-for-all-blockchains/

Adding ID is trivial once domain is implemented, true, but more tech support for extra functions isn't trivial. And there may be other unforeseeable issues. So we will be rolling out new namespace types gradually, with a lot of testnet testing, then public working tests, and time for feedback before implementing each next one.

==-=

MeowBit will be reborn as MeowBip, and incorporated into wallet folder, and set to run with the wallet, to have built-in file resolver with first release of Dot-Bip registration system. User will be able to turn off "run on system start" for both wallet and MeowBip from within the GUI wallet, but default will be on:true.

FYI, MeowBit website:
http://www.meowbit.com/

MeowBit on GitHub:
https://github.com/Derrick-/MeowBit/tree/master/dotBitNS

==-=

Size of text allowed: 520 bytes

Pegging price of bips needed should be done by pinging API of several exchanges that offer BipCoin to BitCoin and averaging them, but should ignore any that cannot be contacted at that moment. Should not give error messages for exchanges it cannot contact.

-=-=-=-=-=-=-=-=-

FUNCTIONS TO INCLUDE IN LATER RELEASE:

--REGISTER FIRST INSTANCE OF CREATION
(Like patent, copyright or trademark, without the government b.s. And only *proves* first creation, does not include any *enforcement*, other than ridicule for anyone claiming THEY first created it.)
Date and approx time of registration will be verifiable buy block height of registration.)

--ID

-SSL REGISTRATION
For SSL, we don't need to use 1024-4096 byte spaces, and that would lead quickly to blockchain bloat.

When displayed for human inspection, fingerprints are usually encoded into hexadecimal strings. These strings are then formatted into groups of characters for readability. For example, a 128-bit MD5 fingerprint for SSH would be displayed as follows:
43:51:43:a1:b5:fc:8b:b7:0a:3a:a9:b1:0f:66:73:a8

ssh fingerprint for a public key could look like this:
SHA256:jP0pfKJ9OAXt2F+LM7j3+BMalQ/2Koihl5eH/kli6A4

There are other short methods also. Any of these could easily fit without bloat.

-MULTI-PARTY SIG ON REGISTRATION OR EXECUTION OF ANY OF THE ABOVE.

-WORDPRESS CAPACITY, to make it easier for everything in WordPress to display properly.

-CHAIN ALL THE THINGS. Pretty much "the sky is the limit." All this and more:
-Dot-Onion support
-IPv6 support
-Messaging systems
-Notary/timestamp systems
-Alias systems
-Issuance of shares/stocks
-Allow zone file support to have multiple domains on one IP
--Cyrillic alphabet, Greek, simplified Chinese and other non-ASCII domain name registration

-=-=-=-=

DOMAIN REGISTRATION **example.bip:**

These are the commands for CLI. All this will be done automatically in GUI.
Delegate your domain and subdomains to DNS servers:

Recommended: * {"ns": ["1.2.3.4", "1.2.3.5"]}

Command	Fee	Transaction fee	Summary	Notes
name_register	***200 mg of gold in BipCoin***	Tiny fee - .001 bip at this writing, may go down	Create domain name. Name becomes public.	You own the domain during the next 478,800 blocks (~12 months.)
name_renew	***200 mg of gold in BipCoin***	.001 bip	Update name	Gives you another 478,800 blocks of ownership
name_transfer	***200 mg of gold in BipCoin***	.001 bip	Transfer name to another address	Gives new address 478,800 blocks of ownership
name_update	***20 mg of gold in BipCoin.***	.001 bip	You update the IP address on a domain.	Changes IP for remaining registered blocks of ownership.
name_always	***5 grams of gold in BipCoin.***	.001 bip	The name becomes yours for all time.	You own the domain during the next all blocks (all *infinity* months.)
id_register	***200 mg of gold in BipCoin.***	.001 bip	Create ID name. Name becomes public.	You own the ID during the next 478,800 blocks (~12 months.)
id _renew	***200 mg of gold in BipCoin.***	.001 bip	Update ID.	Gives you another 478,800 blocks of ownership.
id _transfer	***200 mg***	.001 bip	Transfer	Gives new address 478,800 blocks of

	of gold in BipCoin.		ID to another address.	ownership.
id _always	***5 grams of gold in BipCoin.***	.001 bip	The name becomes yours for all time.	You own the domain during the next all blocks (all *infinity* months.)
(etc. for other services.....)				

(The small transaction fee will go to the miners mining around that time, just like with a payment transaction. The larger will go to development and charity. That is explained further below.)

For future registration functions to be added, the payment formula is this:
Anything that can be squatted (IDs, domain names, Dot-Onion address name associations) will be same price to register and renew as a domain.

Anything that can't really be squatted (registering first instance of creation, unique SSL certs, etc.) will be 1/10the the price to register and renew as a domain. This is 80 cents US at the time of this writing. That's cheap enough for people to easily do, but expensive enough to *heavily* discourage any kind of flooding attack.

Price of registering a document will be 1/8th the price of domain.

Transferring a domain registration or document registration to another address will be the same price as registering a document.

Price of registering an ID will be the same as registering a domain.

Map all hosts in the domain to one IP address:
{"ip":"1.2.3.4", "map": {"*": {"ip":"1.2.3.4"}}}
Example: ./bipcoind name_update d/<name> '{"ip":"1.2.3.4", "map": {"*": {"ip":"1.2.3.4"}}}'

(Above adapted from Namecoin. We could easily use our own code, and names for actins if there is a reason to.)

What this comes down to is very simple. It's two things:
Domain Name:IP Address.

And can easily be updated via the wallet if your website's IP changes.

-=-=-=-=-=-=-=-=

All websites and IDs will be automatically covered by the BipCot NoGov license. Default will be on, but there will be a switch flag to turn that off.

Default will also be to allow "libertarian indulgence" BipCot (low-level non-violent government employees like mail carriers, school teachers, and future-Snowden tech worker bees will be allowed to use the licensed media, but politicians, and violent government employees still cannot use it. Examples: 3-letter agency goons, and law enforcement of any kind.

If libertarian indulgence is turned off, NO employees or contractors of any government can use the thing being registered Dot-Bip, even low-level non-violent government employees like mail carriers, school teachers. This is not recommended. Otherwise, how will those people learn to get REAL jobs?

bipcot_on_yes:true
default: indulgence:on

We will include a simple HTML page (with any small images local in a folder in the wallet install) with a list of our initial Dot-Bip domains and links, so people can test that they've correctly got everything working.

-=-=-=-=-=-=-=-=-=

JSON ATTRIBUTES

--DOMAIN REGISTRATION
domain.bip:ip:true:on

EXAMPLES:
bipcoin:167.114.13.200
forknote:192.30.252.153
cryptonotepool:5.189.135.137

BipCot license on, libertarian indulgence permitted.

--ID
id:meaning

EXAMPLES:
tom:Tom_Smith:true:on
(Tom Smith, will talk to low-level government agents and say "hi" back if they say "hi."

MDC: true:off:Michael's cats BipCat, Beast and Bob.
(Cats CANNOT be petted by ANY government agents.)

bipcot:Beastlick_Internet_Policy_Commission_Outreach_Team:true:off

(Beastlick Internet Policy Commission Outreach Team, all products can NOT be used by *any* government agents.

--FIRST INSTANCE OF CREATION
NameOfThing:URL,MD5,words:file_size,v,true,off
(this uses commas, not colon, since colon can be in web URLs)

EXAMPLE:
DotBip_Whitepaper,c,https://www.bipcoin.bip/ASSETS/wp.pdf,
37203526cb8c6f529a9160b4a649065c,7102,339322,1_1,yes,yes

This breaks down to:

-Name of document to be registered, or Name of document describing first instance of creation of something to be registered:
DotBit Whitepaper

Is document being registered, the thing described in document, or both
(as a, b, or c)
c
(both, i.e. the document, and the thing described in the document, are being registered)

-URL / file path of document:
https://www.bipcoin.bip/ASSETS/dbwp.pdf

MD5 of document:
37203526cb8c6f529a4160b4a649065c

Word count of document:
7102

File size of document:
339322 bytes

Version of document: 1_1

Document and thing described registered BipCot NoGov License: yes
"Libertarian indulgence" BipCot exceptions permitted: yes

As we add new capabilities, the namespace will be added to our enforced syntax. Having an enforced syntax will provide additional help to prevent squatting, "blockchain graffiti" and thus keeping down blockchain bloat.

This will be for now, and may change later at some point.

It will take some time to find the right balance between enabling new features to be implemented, and having a blockchain that's too heavy to early.

These restrictions from the start will not prevent people from creating services around BipCoin that do not directly involve altering the blockchain in new ways.

-=-==

WordPress plugin for our friend Anthony
https://github.com/anthonylv
to make later:
Plugin that automatically correctly resolves all internal in WordPress links via Dot-Bip (harder than just resolving front page of Dot-Bit domain. Plugin would make it easy.

(He's also going to make a WordPress plugin before that, that will make it easy for webmasters to add "donate via BipCoin" function, once we add association for
bipcoin:address
into installer.)

-=-==-=

Some code we'd need exists in Namecoin. We will not use anything NEAR all of it use all of it. Strip it down to basics. Put in fancy stuff later (including fixing their beta of resolving onion addresses securely via TOR bundle). But we'd never use *most* of their code. And we'll write a lot of our own.

We already have resolver (MeowBit) that Derrick made for Namecoin, easy to fix to work for Dot-Bip.

Another reason squatting isn't such an issue: Tell people not to worry so much about exact name. People very rarely type in domains any more, almost always getting to a site from a link or from a search engine. (And Dot-Bip search engines would likely spring up as third-party services. And it's possible support could get added to some existing search engines.)

Like if you wanted cryptonotepool.bip but it is taken, get any of these:

thecryptonotepool.bip
cryptonotepools.bip
cryptonotepoolz.bip

Domains should not be case-sensitive, so all these would work for the same site:
bipcoin.bip
BIPCOIN.bip
BipCoin.bip
Bipcoin.bip

-=-=-=-=-=-=-=-=-

License for Dot-Bip software same as BipCoin: The BipCot NoGov license
http://bipcot.org/
the Namecoin code has the MIT license, which is permissive, so we can use any of it and re-license BipCot, with attribution.

Namecoin core code is here:
https://github.com/namecoin/namecoin-core

Misc;
Someone would invariably build web-based resolvers (sort of defeats the propose but is easy to use for noobs to spread the idea. Maybe not though, or maybe charge a fraction of a bip to use it somehow. It can contribute to DDos amplification:
https://wiki.namecoin.org/index.php?title=HOWTO_Setup_Public_DNS_Resolver

Could Dot-Bip be spread across several coins? Not different TLDs but somehow implementing the same one, checking with other networks before registering? Or would that be a nightmare? We would not implement this, but we could encourage adoption by other (existing and new) coins.

Basically this would be registering via BipCoin, but other coins would update and hold our updated list once an hour to strengthen the Dot-Bip network.

Other coins could also adopt MeowBip for their coin and put in their GUI wallet. So people who don't like BipCoin could still use the Dot-Bip domain system on Bytecoin or Karbowanec. (Or non-CryptoNote coins too.)

If their coin is not licensed BipCot NoGov, they should publicly issue themselves a BipCot libertarian indulgence in order to use Dot-Bit software in their coin.

=-=--==-=
WHAT HAPPENS TO THE BipCoin USED TO REGISTER DOMAINS?

We're going to pay it via one hard-coded address to the core members of the BipCoin team at the time of this writing. They will use half to pay themselves and any additional team members or contractors to keep this thing going.

(Each BipDevs' share within the team will be based on amount of work done and what percentage they contributed to each milestone. i.e. not how many lines of code they wrote but how much they actually solved problems. Payment will be based on quality not quanity.)

The other half of the registration BipCoin (after initial testing and release of the software to the public) will go to these charities:

-- FreeRoss.org (Legal Defense, and awareness outreach for Ross Ulbricht of the "Silk Road.")

-- Antiwar.com (Anti war education.)

-- FIJA.org (Jury Nullification and outreach.)

-- Restore the Fourth / Reinst8 (ending mass government surveillance https://restorethe4th.com/)

We will also provide free lifetime Dot-Bip domains to these organizations, and help them set it up. These will also be links in the "About" tab of the wallet, to click and test that it's working after you set it up.

We picked charities only a loon could not like and picked ones that are international in appeal, not local. Jury Nullification applies largely to US law. But FIJA does some work outside the US, and as an educational organization, is international in scope and appeal. Restore the Fourth is in the US, donations also go to their sister org in Europe, Reinst8. FreeRoss.org and Antiwar.com are entirely international in scope.

We will not be converting BipCoin to BTC to send charities. Part our plan is to encourage adoption of BipCoin. Someone at the charity will need to take three minutes to install a BipCoin GUI wallet. But BipCoin can be converted to Bitcoin on Cryptopia exchange, and we will likely be on more exchanges in the future.

We've talk to someone at all four of these charities, and they're all willing.

We'll pay out to them once a month at least.

The charities and can feel free to let people know if we ever stop paying them, so there is transparency.

After a time, we may add or remove charities, but this is at the discretion of the BipDevs for the first two years after release of Dot-Bip.

BipCoin in the incoming wallet will be transferred out of that wallet once a day. We don't want to keep all coin in one wallet for more than a little time, to make the people holding the keys not be a target for theft.

There will be a vague general accounting of this, but we're not going to spend time with detailed reports of who did what when where. The time that would take is time we could be working. And detailed reporting by person also violates the principle of an anonymous coin.

Our *results* will be our real "quarterly reports." Let the users see that commitment in the code.

This will be the plan for 2 years after release of initial Dot-Bip. Then this topic will be opened up to the public for comment.

This could include options such as paying out some to the miners and how that would be technically implemented, or continuing the situation as is, or adding other charities, or something else.

After 30 days of public comment, this plan will continue for 30 more days while the dev team (basically acting as an ad hoc board) will decide which path to take.

It is very likely that some BipCoin will still go to the dev team and to charity. Possibly additional, or different, charities. And it is possible that some will then go to miners.

People who don't like the final decision can invent their own system. They can use our code and mechanisms, if they are not aligned with any government.

Anyone who is not happy with any of the above should also keep in mind this:
NameCoin BASICALLY THREW ALL INCOMING REGISTRATION COIN DOWN A FLAMING HOLE, then spent years wishing they had funding.

When you registered a domain on Namecoin, *the Namecoin was destroyed*. We hate the idea of that. Also, we *can't* do that, because we're charging more than a trivial amount. So if registering a Dot-Bip address destroyed some coin, eventually all coin would be destroyed and there would be no network to support the system.

Namecoin devs destroyed coin, but then spent the next five years begging hard for someone to help them with their important work, to finance it. I agree with them that they deserved to get paid, but they could have paid themselves the way we are, instead of basically burning all the money they were paid.

Namecoin devs got so desperate they even started to consider things that would undermine the whole system, like partnering with giant corporations

In 2013:
https://forum.namecoin.org/viewtopic.php?f=18&t=1414&
In 2016:
https://forum.namecoin.info/viewtopic.php?f=18&t=2471

There was talk on that forum and in their IRC of partnering with other corporations.

There was even talk from devs on the IRC at one point about trying to partner with ICANN!

This would be like if Satoshi had partnered with the United States Federal Reserve. In other words: completely antithetical to the independence, decentralization, and mission

If the Namecoin devs had partnered with ICANN or even any large corporation to insure the survival Namecoin, it would have lead to the destruction of Namecoin.

SO, BOTTOM LINE ON REGISTRATION BipCoin:
Half the BipCoin from registrations and renewals will go to dev team. We don't want to compromise our work effort and integrity by having to cyberbeg, do constant fundraisers, or make deals with devilish borgs.

The other half of the BipCoin brought in from registrations and renewals will go to some great charities.

OTHER USES FOR THIS SOFTWARE
Our mechanism could be used in other coins for pairing other things to real-world gold price.

LIST OF CODE REQUIRED FOR FIRST PUBLIC PROOF-OF-CONCEPT WORKING BETA
--Code to view Dot-Bip domains system wide already exists, Derrick created it ("MeowBit") for Namecoin and it should be easy to adopt.

--Code to add domain:IP pairs into the blockchain. Should include code to enforce syntax to prevent other text from being added. Let's use IPv4 IP for now, but we will add IPv6 later. So the syntax allows will be letters/numbers (and no spaces) up to, let's say 256 characters for the first part, and numbers only in any standard IPv4 octet for the second part. *Except for the enforced syntax, this code exists in Namecoin.*

--Code to figure the current price of registering, in bips, based on price of gold from the gold API we have permission to use.
Should check gold price once a week and should check BipCoin price every eight hours.

--Code to compare the above two to determine price in gold/dollar/bip.

--Code to allow domain:IP pair to be added only after payment is made. *This code already exists in Namecoin and can probably be adopted for BipCoin.*

--Code to reject blocks that have registrations in too-low gold prices. (Search "PREVENTING CRACKING" in this document above for more on that.)

--Code to pay BipCoin for registrations coming in out to one hard-coded address (will be paid from there to charities and devs). Should have some mechanism to prevent someone compiling our code, and changing that address. i.e. some how blockchain must authorize each one. Maybe should only pay out once an hour to reduce stress on network.

This mechanism could maybe include Derrick's Blockchain Notification System**,** the feature that Derrick added for Notification from Dev to users, alerts via blockchain. (Could also maybe be used for mechanism to broadcast price of BipCoin to network?)

http://www.meowbit.com/meowbit-now-with-update-alerts-over-the-blockchain-a-new-feature-for-all-blockchains/

This address could eventually be a multisig address, but for now let's just make it one address.

--Code to update IP addresses, renew domains, and transfer to another address. *This code already exists in Namecoin and can probably be adopted for BipCoin.*

--Hard code in a few address:IP pairs for devs, of our websites. Could be criticized by some as a sort of "pre-mining", but we're not squatting names to sell, we're registering names we'll use. Including names related to this project.

It is basically also to show test demonstrations upon installing software to make sure it's working. Would be registered for all time, but IP would be able to be updated normally, and could be transferred normally to another address if needed.

IN CONCLUSION

Henry Ford didn't invent the internal combustion engine, nor was he the first person to put one on a carriage to make it work without a horse. But he put a car in every carriage house. And when he started most people had never even *seen* a car.

He made cars practicable and affordable. We plan to do this for distributed, difficult-to-censor DNS.

Namecoin established some amazing ideas.

But BipCoin will take these ideas and make them easy to adopt for everyone.