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 v1.115
12/14/2016

Indiegogo fundraiser: https://igg.me/at/dotbip

Whitepaper written by MWD with some input from other BipDevs (BipCoin dev team members.)
First draft was published on Nov 25, 2016.
bipcoin@gmail.com
https://bipcoin.org/

Abstract:

Background: "DNS" is the method by which website names (like "google.com") are registered and can then be used by everyone to get to a particular website. This registration system is monopolized worldwide by a US Government-controlled organization. Thus domains can be censored and seized by simply rerouting them. These take-downs occur often, and are frequently executed without any due process whatsoever.

This is unacceptable, and antithetical to free speech. It also can ruin someone's livelihood. People work for years building an online business, only to have it destroyed by some bureaucrat in a cubicle not liking it.

In 2011, there was an attempt to make a parallel system that was not controlled by governments. This system registered domain names on the blockchain of a Bitcoin-like cryptocurrency called *Namecoin*.

Namecoin worked in a theoretical way, but never got any adoption at all for distributed DNS. This was because it had too many problems. These problems are etched so deep into the very backbone of Namecoin itself, that it is unlikely the Namecoin developers will ever solve them.

Results: We have identified all the problems that kept Namecoin from adoption, and we've solved all these problems on paper. Now we just need to implement them.

Conclusions: With the right help (financial contributions plus a couple more programmers), we can solve these problems quickly and have a system ready to be easily adopted by even the most technically unsophisticated people. Additionally, we will do this in a way that people will *want* to adopt it. And we will be building it on top of our existing cryptocurrency, BipCoin.

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

(Short form) 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 included from day one of Dot-Bip

--Domain resolver for Dot-Bip is SYSTEM WIDE

--Domain resolver Dot-Bip will work for tech noobs

--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

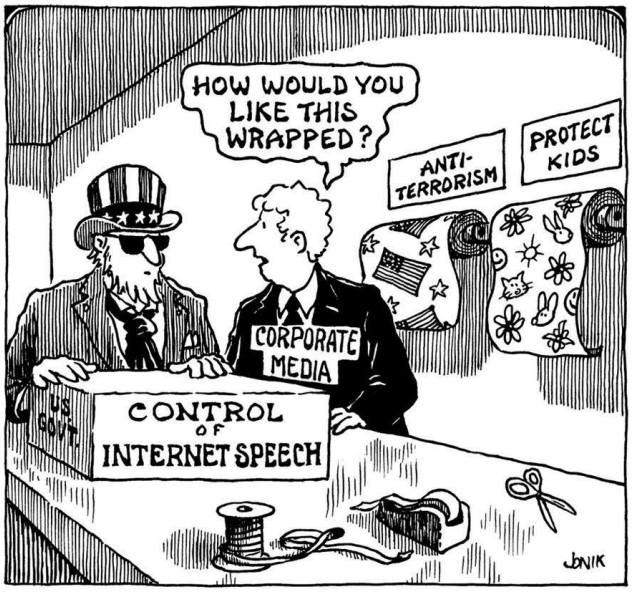
--Dot-Bip will pre-solve the security issue that was discovered in Namecoin

--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 from the control of governments that can outlaw any type of free speech at a whim...or with the election of a new "leader."

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 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 even 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, and also studied their work, words and actions. The BipDevs have also extensively studied the distributed DNS problem in general.

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 that 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, this registering happens automatically and happens on the blockchain. It does not involve some company or person doing something for you. It involves the user making a Namecoin payment and entering some information into the Namecoin wallet. It can happen while every member of the Namecoin team is asleep, and it works pretty quickly.

Users initiate 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 when you send any cryptocurrency to someone else.

It really is a brilliant idea. The idea predates the Namecoin team[1], but kudos to them for making it sort of work. (Kind of. Maybe. I'll give them this: they made it work in a "this works in a laboratory setting" way, and that is one step beyond theoretical. But five years later, no one is using Namecoin in any real-world usages other than buying and selling Namecoin. And there are 640 other cryptocurrencies you can buy and sell on exchanges.)

The Namecoin DNS system top-level domain, Dot-Bit (.bit), is not accessible from normal browsers without special add-on software.

Users who have that special software, plus the Namecoin blockchain on their local machine, or a website 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 normal domains can be taken down by government agencies demanding that the domain registrar essentially un-register the domain or point it to a "this domain has been seized" placeholder page on some government computer.

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 (another Namecoin address) easily and securely from within the wallet.

Much of this will work the essentially the same in BipCoin's Dot-Bip, 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.

---

[1] The idea of uncensorable DNS on a blockchain actually goes back to a Bitcointalk.org forum post by a little-known user named appamatto, here https://bitcointalk.org/index.php?topic=1790.0

Appamatto proposed doing it on the Bitcoin blockchain.

Satoshi Nakamoto, creator of Bitcoin, chimed in on the conversation. He liked the idea, but he suggested doing it on a different blockchain. He suggested also "sharing CPU power" with Bitcoin: https://bitcointalk.org/index.php?topic=1790.222

So Satoshi not only created Bitcoin, he also, in one post, created the idea of altcoins and merged mining!

The Namecoin guys just did some coding on this, then did everything else wrong. Because they all were all math all the time, and no one on their team worried much about *adoption*. Namecoin is still traded today mainly because of its historical value as the first altcoin.

> 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.
>
> -=-=-=-=-=-=-=-
>
> NOTE: In parts below where we talk about doing Dot-Bip on *the blockchain*, we are talking about the BipCoin blockchain, not the Bitcoin blockchain, not the Namecoin blockchain, and not any other blockchain. That should be obvious. But it might not be obvious to some non-tech people who have heard about this mythical thing called "THE blockchain."

(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.

This was so cheap that someone mined a little Namecoin (back when it was easy) and used a bot to Dot-Bit register every noun in the English language! This happened within a few months of the release of Namecoin. This made it virtually impossible for people to get the domain they wanted.

Dot-*Bip* addresses for a domain or ID via *BipCoin* will cost 8 USD (in late 2016 dollar value) of BipCoin for approximately one year, or 200 USD 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).

> Registering a Namecoin Dot-Bit address has always been 9 months at a time, not one year. 9 months is too short. It also makes is hard to remember approximately when you need to review your domain. So with BipCoin's Dot-Bip, we've increased that from approx 9 months to approx 12 months.

Registering a Dot-Bip domain will not always require the same amount of BipCoin. That will vary, unlike with Namecoin. But the amount of gold required to buy the BipCoin needed to register a domain will stay the same. More on how we'll achieve this later. But basically we've found a decentralized way to hard-code peg the number BipCoin to register a domain to the price in gold at that time. It will always be the same amount of gold, which will be a different amount of BipCoin, depending on the prices of gold and BipCoin.

--**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.)

--**Our domain resolver *MeowBip* for Dot-Bip is SYSTEM WIDE**, not for one browser only as with FreeSpeechMe for Namecoin. Namecoin's FreeSpeechMe only worked on www, and only via Firefox.

BipCoin's MeowBit resolver will make ANYTHING on your computer able to resolve a Dot-Bip address. That includes *all* browsers, e-mail, FTP, IRC, Pidgin, etc. (And we already have *this* section of code written, because we wrote it for Namecoin a few years ago.)

--Domain resolver MeowBip for Dot-Bip is easy to use for everyone, not just tech people. And it will run in the background, invisibly, unlike Namecoin's FreeSpeechMe.

Namecoin's resolver, FreeSpeechMe, was not easy to use for non-technical people, and it crashed. And the *horrible* Namecoin wallet that had to be running *took ten minutes to open* before it would begin syncing the blockchain(!)

This turned off all but the most dedicated and stubborn "I ***WILL*** GET THIS TO WORK" users. That does NOT encourage adoption.

--**Our 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 are easy to create and maintain from information about the network. This information is already displayed now in our CLI wallet. Will make developing Android / iPhone wallets and wallets for tablets and other mobile devices very doable, since they won't need to carry the whole blockchain.

Also, it was a great failure over all of Namecoin that you had to have the whole node to resolve domains. No one wants to lug that around on their phone or even a desktop computer. This could use a Merklix Tree. (Not a typo, and more on that later.)

Then there wouldn't be as much of a need for web resolvers like this one for Namecoin: https://bit.no.com/

Though those wouldn't hurt to run. The more adoption and ways to view a Dot-Bip site, the merrier. And we (or a third party) could easily make software to make it easy for people to run these as a part of BipCoin node. It could even be included as a part of the BipCoin software.

Some public DNS servers also start to support Dot-Bip.

Same with alternative network information centers, like OpenNIC.

--**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 their open-source software without checking with Namecoin devs first. lol.

OneName gave up on dealing with Namecoin and moved their project over to the Bitcoin blockchain, and it is being used today as a result.

--**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.

BipCoin Dot-Bip domain registration, and resolving of domains, will be built into our GUI wallet. Our GUI wallet works well and opens in seconds. And it will be easy to register, transfer and resolve domains for people who do not have any technical understanding. We also have written, and will continue to write, extensive, easy to use tutorials for all features.

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

OK, NAMECOIN'S DEAD. BUT WHAT ABOUT _____?

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 systems, working or theoretical, deal well with the domain squatting problem. Some tried to deal with it by making people *bid* on domains, which drives the cost out of reach for most people.

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

> The problem with most of these systems, and a lot of software in general, is the teams are all engineers, or all engineers + marketing weenies.
>
> The BipDevs have one person on the team who is not a programmer. He's a tech writer, end users, and a first adopter user of a lot of systems, since the Internet began. So he sees the bigger picture. He can make himself see things the way a noob would see things.
>
> This is what most teams don't have: the guy asking "Why would anyone in their right mind want to *use* that system?" before engineers start coding the system
>
> (It's the guy writing this whitepaper, in case you didn't already guess.)

None of these DNS solutions have much/any adoption. **Adoption is the key**. Without widespread adoption, any service that claims to offer DNS is just a theory put forth by theorists, even if there is "working" code.

And that includes Namecoin. And Emercoin.

Many other 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 an end user? There may be a few geeks reading this who know one or two people doing this, but that is *not* adoption. We believe we can make this easy enough to use and at a reasonable registration cost 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 blockchain 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 really has been yet.

I mean, there is TOR, which makes sites hard to censor because it's hard to find where they're hosted. But TOR is hard to use for webmasters and users. And it's even harder to use correctly.

There is a theory that Ross Ulbricht is in prison 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 new incoming regime in the USA - a president who has vowed to silence journalists - censorship-proof internet that's easy to use will become very important very very quickly.

We don't have it in place and we *need* to have it in place. Dot-Bip can achieve this.

Not that it would have been much better under Hilary, she is practically owned by bankers and has used dirty tactics to silence her critics: 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 in how tyrannical different politicians are is 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:[2]

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.

Read 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!

FFAQ (Future Frequently Asked Questions):

[2] It may seem that the BipDev writing this whitepaper has it out to bash Namecoin and the Namecoin devs. However: 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 many many 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.

Another example: the Namecoin devs once let **namecoin.bit** expire! Their flagship proof-of-concept domain! This happened because they were so disorganized they couldn't remember which dev tem member was in charge of it. This is covered on Namecoin dev tem member indolering's blog, here:
https://www.indolering.com/domain-name-squatters
(And yes, we have screenshots of all these, in case anyone starts throwing history down the memory hole.)

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.

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

Dot-Bip Domains are not case-sensitive, but you get the idea. And you can write them that way to make them easier to read and remember.

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
Fun.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
BestFun.bip
etc.

Like if you wanted
cryptonotepool.bip
but it's already 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

It is our opinion that there was way too much overvaluation of ICANN-based 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 yet 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.

Domain names are still incredibly important. People don't type in domains that much anymore, often getting to a site from a link or a search engine. But for a search engine, they need to be able to remember the name of the site, at least close enough for someone to have the search engine correct them. And people use domain names a lot when sharing links with friends, on social networks and in emails and texts.

(A lot of systems won't even *resolve* a raw domain address, seeing it as some sort of security attack.)

And Dot-Bip search engines would likely spring up as third-party services. And it's possible Dot-Bip support could get added to some existing search engines.

But people need to remember domains, and need to have something to bookmark other than an IP address.

WHAT IF NAMECOIN JUST STEALS YOUR ANTI-SQUATTING IDEA AND IMPLEMENTS IT?

Well, it wouldn't be stealing. And they're welcome to try, because they couldn't pull it off. Too many of their domains are already squatted. Plus after five years, they still don't have an easy way for noobs to resolve domains.

WHAT IF SOME OTHER COIN JUST STEALS YOUR ANTI-SQUATTING IDEA AND IMPLEMENTS IT?

Well, it wouldn't be stealing. But if someone actually makes it work and it gets adoption, excellent. We'd just help support that. Seriously, we *just want to see this happen* and get widely adopted before it's too late.

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-programmer driving everything, that other teams don't have. Ideas cannot be "stolen", especially if they involve *you* as an integral part of the equation.

SO HOW WILL Dot-Bip 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 (value actually) of a cryptocurrency itself to gold, but *that's not how this works*. Devs don't get to say "our coin is worth X." That's the job of the market.

The Dot-Bit part of the BipCoin daemon will average BipCoin cost on all exchanges that currently take BipCoin and use the price in dollars or euros. So registering a Dot-Bip domain for one year is always 8 dollars US worth of gold worth of BipCoin at time of this writing (in rounded off early November 2016 value USD and gold prices).

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 in general, but especially after the recent USA election.

Gold is also just a better stable commodity in general. The value/price remains close to the same, even as the cost rises. i.e. 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 prices are not terribly common, many charge money to use them, 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 could work. But we'll shoot for once a week, the one week 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 cost in an hour, and repeat this until it found the new price.

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.

One precious metals dealership has already allowed us to use their API for gold price for the initial roll out, but we will need more eventually, to go beyond proof of concept.

> NON-API ALTERNATIVE: If we can't do this with APIs: and even if we can, this method would be preferable:
>
> Make the daemon do a quick web search and find the price of gold. Type
> **Gold price in US dollars per ounce**
> (in English, and not in quotes) into any search engine that uses any language, doing the search from any country, and many results will have the current price of gold, displayed on that page without even going to any of the links.
>
> We could get the current price of gold by auto-searching from a text list of every search engine (there are a LOT more than just Google), and having a little bit of code that basically scans all the text returned for *numbers preceded by a dollar sign*, and averages the numbers that are within 10% of each other (discarding anything after a decimal point, because it's not needed). That would undoubtedly return the current price of gold or very close to it. Close enough for this.
>
> The same could likely be done for the price of BipCoin when BipCoin becomes more popular, though it probably wouldn't need to be done. Cryptocurrency exchanges usually are more inviting about using their APIs for third-party services than gold price listings are. Some Gold price listings may be likely to block traffic from BipCoin since we would not be paying them.
>
> The five search engines used each time would be picked randomly from a list, so it's not the same ones over and over.
>
> Using this method AND a set of APIs would probably be best. More redundancy is always good.

The price of gold is stable(ish) enough that the idea is really just to get a price that's not wildly off. 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, MeowBip via BipCoin will still allow *viewing* any previously registered Dot-Bip domains.

The BipCoin daemon should not give error messages that will be seen by the casual user for exchanges it cannot contact. These should only show for troubleshooting. Thus these errors should only show if user sets log level to higher than default.

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 checked 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 for everyone 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 BipCoin 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 if our daemon has more than one IP to access each exchange, when available.

This system makes sure no one is changing the code and cheating it to mass-register many domains

Our system will even work with large rises or falls in the price of gold.

While gold is generally stable overall compared to many commodities, 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 many-decade gold price data is available here:
http://www.kitco.com/charts/historicalgold.html

To hack our system someone would have to change all the other nodes code, not just their own. This becomes closer to impossible as more nodes are added.

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 into 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 correctly 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 free speech and free commerce becomes illegal), the updated code could be reviewed by people, then compiled from those repositories to avoid backdoors. And as long as the new software were adopted by most miners and nodes, it would work.

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

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

i.e. if gold were the price of steel, registering a domain would cost about 200 pounds of gold's worth of BipCoin. Lol.

WHAT IF THE PRICE OF GOLD DOES *NOT* STAY STABLE?
Let's say some newly elected billionaire president of a nation with a major world 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.[3] So he outlaws ownership of gold, thus making gold black market and having wider price fluctuations?

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

A cost 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 value fluctuations like Namecoin had that we are avoiding with this system. Actually we only need to stay in the same order of magnitude. Namecoin went *way* out of this range.

Namecoin made it a set amount of coin to register a domain. Namecoin's cost has varied 4500% from lowest to most expensive quickly, and is back down near its lowest now.

So registering a Namecoin domain started out so cheap that someone squatted every English word as a domain, went 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 cost of registering a Namecoin domain has historically had a hyperinflation rate approaching that of 1923 Germany's Weimar Republic, where people were burning 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 traded and mined. It's new enough to not be too difficult to mine, but not so hard to mine that people without expensive mining rigs won't mine it. And the BipCoin network has enough hash power to make transactions work very well. This cannot be said of many altcoins. And hash power of any brand new coin could start at zero.

Put it this way: BipCoin transactions confirm faster than Bitcoin 100% of the time. Sure, this is partly from BipCoin's 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.

[3] It's not without historical precedent. Socialist hero FDR outlawed private ownership of gold from 1933 to 1934. Many people were jailed for owning something that had been legal the day before. For more info see https://en.wikipedia.org/wiki/Executive_Order_6102

And unlike some new corporate blockchain contenders for creating everything (including distributed DNS), BipCoin has never had some huge spilt that lost people millions of dollars and fiercely divided communities.

BipCoin is also a *known thing*. It's traded. It's on an exchange. It's on the CoinGain Currency calculator website. It's on market cap websites. CLI and GUI BipCoin wallets exist already for Windows and Linux. And we plan to add Mac support after the Dot-Bip beta is finished.

There is extraordinarily detailed tech documentation on the BipCoin website that makes it easy to use 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. And all of the dozen or so CryptoNote coins are either too far along to add something new without being perceived as huge mission creep, or else they do not have the use, adoption, price and following of BipCoin.

> NOTE: If Dot-Bip gets adopted it will likely drive up the cost of BipCoins. So mine some now and/or buy some on Cryptopia while they're cheap. (Not a guarantee of performance. At all. In any way. Just a thought).
> https://www.cryptopia.co.nz/Exchange/?market=BIP_BTC

WHY NOT DO THIS ON BITCOIN'S BLOCKCHAIN INSTEAD?

Bitcoin has a huge bloated blockchain already, and sometimes even has problems confirming transactions. I had a small Bitcoin transactions take two days recently (!), even using the default fee in MultiBit.

Plus there are large arguments as to what to do with varying technical aspects of Bitcoin (witness the advent of Segregated Witness, pushback against it, and the continuing block size war that is not even solved with SegWit.

.And people are *religious* about Bitcoin and *married* to Bitcoin…to where if you try to do anything that actually puts data repeatedly on the blockchain, people get furious.

BipCoin does not have any of these problems. And remember, the original suggestion on Bitcointalk.org was to do distributed DNS on the Bitcoin blockchain, but the creator of

Bitcoin chimed in and suggested against that. He saw a lot of where the future of Bitcoin could go, this is obvious from the fact that Bitcoin has even scaled as well as it has, and that the network itself has never been hacked….No one has ever created a false transaction on mainnet and had it stand.

Also, BipCoin is based on CryptoNote, so it has truly anonymous transactions, unlike Bitcoin. This will also be true of any registration capacity we add to BipCoin.

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 cost of BipCoin in dollars or euros.

When Dot-Bip becomes commonplace, it's likely that our mechanism could be used in other coins for pairing other things to real-world gold price. Eventually many cryptocurrency exchanges would have a drop-down option on their website, and an option in their APIs, to read the price of a coin in milligrams of gold, along with the current prices shown in Euros, US dollars, Pound Sterling, Yen, millibits, etc.

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 precious 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.

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, which will help the health of the whole system.

This may also encourage people to watch BipCoin closely to find the right moment to register. People also might develop services to try to find the perfect moment to register.

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 need 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 the BipCoin 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.

Our software is on GitHub, but subsequent releases with source code will also be released as torrents so even if the source were removed by force 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."

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 exchanges each, would be harder to censor than an ICANN-controlled domain.

Most things called "decentralized" are actually just "distributed" on a large scale. This includes Bitcoin, where a steering committee 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.

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 two-dozen people control decisions* of what is and isn't adopted in Bitcoin, which is the most "decentralized" technological and economic system in history.

We're really concerned less if Dot-Bit meets the academic definitions 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
https://en.wikipedia.org/wiki/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 the domains, even if just as emergency backups for ICANN-registered sites.

--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 Dot-Bip beta 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.

MECHANISM FOR CHECKING BipCoin PRICE
We add a random number generator in daemon that would determine a period in the first hour of the 8-hour window for every instance of software to check the exchange(s) for the current cost 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 eight-hour period, then checking stops.

Then all other daemon instances on the network are told *not* to check (if their time hasn't come up yet).

The random number generator would keep all wallets from checking at once and overwhelming the exchange(s) and our network.

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 240 blocks, and no other daemon instances should check the price during this 240 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 Namecoin we only used it to signal wallet owners when there was an update to install.

Eight-hour time is approx. Actually would happen every 240 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 bip 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.

Here's something like that for Namecoin's Dot-Bit. It's a website that alerts you when your domain is about to expire:
http://namealert.mvps.eu/

Though that service is free. There could be similar services for BipCoin's Dot-Bip that charged a tiny bit of BipCoin. They'd have more incentive to not go out of business.

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

FUNCTIONS THAT WILL BE POSSIBLE UPON RELEASE:

--Domain registration

--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

-- Derrick's Blockchain Notification System**, the feature that Derrick added for Notification from Dev to users**, alerts via blockchain. This would be probably only if needed as the mechanism to broadcast the current cost of BipCoin to network: http://www.meowbit.com/meowbit-now-with-update-alerts-over-the-blockchain-a-new-feature-for-all-blockchains/

That's it for the beta. Adding ID is trivial once domain registration is implemented. But extra tech support for additional 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 beta tests, and time for feedback before implementing each next one.

Size of text allowed: 520 bytes

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

FUNCTIONS TO INCLUDE IN LATER RELEASES:

--REGISTER FIRST INSTANCE OF CREATION
Described at length 4 pages further ahead.

--ID
A shortening of a name or identifying phrase. Like two or three letters might be registered to stand for that persons full name or company. Could also be used to stand for a Bitcoin, BipCoin or other address (Like OneName does with Bitcoin.)

--Signing documents
A verifiable identity. Or at least verifying that you have the private keys and password to the wallet that created an specific identity.

--SSL CERTS
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

The 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 in the Dot-Bip version of a website. WordPress blogs are more than 24% of the entire web, so they need to be accommodated.

It's easy to make the first page on a Website display with Dot-Bip. It can be hard to make all the internal links and images work properly in Dot-Bip.

We encountered this with Namecoin's Dot-Bit. There is a clunky workaround for webmasters to add some code into their wp-config.php file, but it doesn't always work on everything. This should be addressed with a WordPress plugin for non-techy WordPress blog owners. But it could also be helped a little bit from the Dot-Bip side.

--CHAIN ALL THE THINGS
Pretty much "the sky is the limit." All this and more:
-OpenBazaar address support
-Dot-Onion address support
-IPv6 support
- Human memorable names for data locations on intranets
-Messaging systems
-Notary/timestamp systems
-Issuance of shares/stocks
-Allow zone file support to have multiple domains on one IP
--ZeroNet name support (https://zeronet.io/)
-- Osiris name support (http://www.osiris-sps.org/)
- Syndie name support (https://www.syndie.de)
--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 BipCoin 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 of gold in BipCoin.***	.001 bip	Transfer ID to another address.	Gives new address 478,800 blocks of ownership.
`id _always`	***5 grams***	.001 bip	The name	You own the domain during the

	of gold in BipCoin.		becomes yours for all time.	next all blocks (all *infinity* months.)
(etc. for other services.....)				

The small transaction fee of .001 bip will go to the miners mining around that time, just like with a payment transaction. The larger amount 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 eliminate 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"}}}'`

(Some of the above adapted from Namecoin.)

What this largely comes down to is very simple. It's mostly just things:

Domain Name:IP Address.
or
ID:full phrase
etc. etc.

Sometimes there will be a little more included….

All websites and IDs registered Dot-Bip 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. Basically anyone who carries a gun for the government, or directs, allocates or funds the government guns.)

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 setting is not recommended. Otherwise, how will those people learn to get REAL jobs?

If a license other than BipCot is used, use
`bipcot_on_yes:false`
`default: indulgence:na`
(the "na" is for "not applicable.)
and put the license you want on the website you're registering, in a place that's easy to find.

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

JSON ATTRIBUTES

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

EXAMPLES:
`bipcoin:167.114.13.200,true:on`
`forknote:192.30.252.153,true:on`
`cryptonotepool:5.189.135.137,true:on`

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", but not much more.)

`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:t
rue: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,MWD,c,https://bipcoin.org/ASSETS/WP/Dot-
Bip_whitepaper.pdf,37203526cb8c6f529a9160b4a649065c,9881,33
9322,1_1,yes,yes
```

> NOTE: MD5 could be replaced with SHA-256 for higher security. We're using MD5 here as an example because it's so embedded in common use for verifying simple documents.)

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

Author of document:
MWD (Full name could be used here, but should have underscores instead of spaces between words.)

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 (on Internet or on an intranet):
https://bipcoin.org/ASSETS/WP/Dot-Bip_whitepaper.pdf

MD5 of document:
37203526cb8c6f529a4160b4a649065c

Word count of document:
9881

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

If a license other than BipCot is used, use this in the JSON:
`bipcot_on_yes:false`
`default: indulgence:na`

(the "na" is for "not applicable.)
and put the license you want on the website you're registering, in a place that's easy to find.

This system could replace patent, copyright, trademark, without the government b.s. and without the blockchain bloat of putting whole documents in the blockchain, like some have suggested. It could also be used to register first sequencing of a particular species' genome.

This system only *proves* first creation, does not include any *enforcement*, other than ridicule for anyone claiming THEY first created it first.)

Our system for registering First Instance of Creation could be useful in defending *against* government-sponsored patent trolls, by allowing people to prove *Prior Art.*

Date and approx time of registration will be verifiable buy block height of registration.

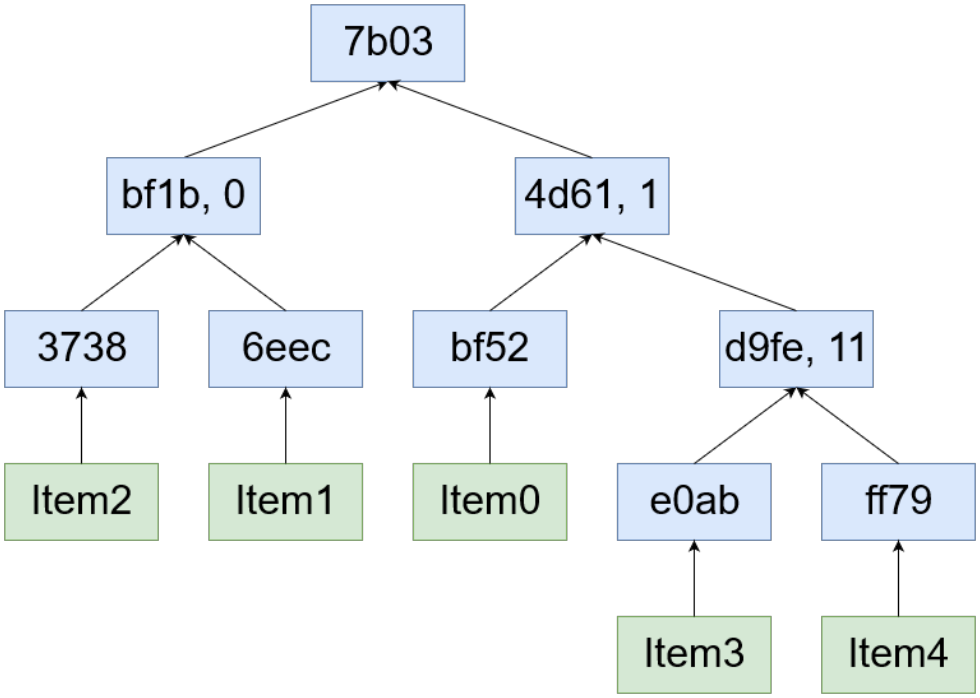
-=-=-=-=-=-=-=-=-

--Light clients MUST be very easy to make and use.

> Chris Pacia from OpenBazaar suggested:
>
> "It's a must-have for any name system to have the state root committed to the block header. Preferably using something like a Merklix Tree. The main failure of Namecoin, in my opinion, was that nodes could not serve lightweight proofs, so it required running a full node to resolve names.
>
> "Anything that requires people to run full nodes will never achieve mass adoption.
>
> "So you need a lightweight proof that the IP returned for a given name is valid... and that it's the *last* valid entry in the chain (which is why you need a state root in the header)."

"A Merklix Tree has faster insertions and deletions than a Merkle Tree."

Merklix Tree is *not* a typo:
http://www.deadalnix.me/2016/09/24/introducing-merklix-tree-as-an-unordered-merkle-tree-on-steroid/



(There is more on that blog from time to time on the Merklix Tree subject:
http://www.deadalnix.me/?s=Merklix&submit=Search

(That article mirrored here: https://bipcoin.org/ASSETS/Merklix_tree.pdf)

NAMESPACES
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.

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 before there is the ecosystem to support it.

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.

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

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.

These can contribute to DDoS amplification:
https://wiki.namecoin.org/index.php?title=HOWTO_Setup_Public_DNS_Resolver

So that problem would need to be solved. Maybe charge a fraction of a bip to use it somehow? (This would only be needed by people without the wallet, using a web wallet.)

Could Dot-Bip be spread across several coins?
Not different TLDs but somehow implementing the same one, checking with other networks before registering? 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 our software is adopted by a coin that is not licensed BipCot NoGov, they should publicly issue themselves a BipCot libertarian indulgence, then shame themselves, in order to be able to use Dot-Bit software in their coin.

=-=--==-=

WHAT HAPPENS TO THE BipCoin USED TO REGISTER DOMAINS?
80% of will pay out once a day via one hardcoded address to the core members of the BipCoin team at the time of this writing. They will use that 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 quantity.)

The other 20% of the registration BipCoin (after initial testing and release of the software to the public) will be split ways 4 to go once a day via 4 hardcoded addresses to these charities (5% each):

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

-- Antiwar.com (Anti war education.)

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

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

We will also hardcode in free lifetime Dot-Bip domains to these organizations, and help them set it up. These organizations' Dot-Bip links will also be in the HTML file included in the install of the wallet, to click and test that it's working after you set it up.

We picked charities only a loon wouldn't 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 of 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 talked to someone at all four of these charities, and they're all willing.

The charities can let people know if they ever stop receiving payments, 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 Dev team 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 general accounting of this, but we're not going to spend time with detailed reports of who did what, when, and where. The time that would take is time we could be working. And detailed reporting to a man also violates the principle of a truly 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 and adding other charities, continuing the situation as is, or something else.

> I'm sure some would say "use it to pay more to the miners!" But paying miners out of registration fees is a bad idea, it would allow bigger miners to have more control over the registering of blocks of domains, which is a bad idea. It centrally concentrates too much power of the network *away* from decentralization.
>
> This idea was discussed with Namecoin and they ultimately decided the best thing to do was throw away the registration fee coin.
>
> It might make sense to pay some of the registration fee to the miners far in the future, when the incentive to mine gets low, once the block reward is very low and there are many people mining with great hash power.

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.

Or if there really is a huge difference in opinion, someone could alter BipCoin Dot-Bip software as you wish. And if you could convince a majority of miners and nodes to adopt your version with your vision, it wouldn't matter what the BipDevs think.

This really is true democracy in action, in an opt-in setting. (Unlike governments, where you are opted in before you can speak, and you cannot painlessly opt out.)

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 and wondering how they could get funding.

> A business plan that doesn't include how people will be paid for their labor is not a business plan at all. Namecoin had no business plan.

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 their paycheck every week.

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 also 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 of Bitcoin that he defined in his whitepaper.

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, THE BOTTOM LINE ON BipCoin USED FOR Dot-Bip REGISTRATION:
80% of 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 20% of the BipCoin brought in from registrations and renewals will go to some great charities.

WHY DON'T YOU SPLIT IT 50/50 WITH THE CHARITIES?
We originally planned that. But a good friend of ours who runs companies and signs paychecks each week for dozens of people read an early draft of this whitepaper and made this suggestion: "Don't shortchange the developers. 20% to charity is VERY generous. The difference between splitting it 80/20 and splitting it 50/50 could very well be the difference between success and failure at some point down the line."

OTHER USES FOR THIS SOFTWARE
Our mechanism could be used in other coins for pairing other things to real-world gold price. This will be even easier after cryptocurrency exchanges start to regularly include the price of a coin in milligrams of gold, along with the current Euros, US Dollars, millibits, etc.

DOESN'T "BIP" ALREADY MEAN SOMETHING ABOUT Bitcoin?
Yes, "BIP" is the acronym for "Bitcoin Improvement Proposals"
https://en.bitcoin.it/wiki/Bitcoin_Improvement_Proposals

But there's no chance for confusion from the general public. That meaning of "BIP" is only used by people who actually contribute code to Bitcoin.

Our use of "Dot-Bip" has nothing to do with that. It's derived from the word *BipCoin* which is named for the license we use on everything we make, the BipCot NoGov license.
http://bipcot.org/

Ask Amir Taaki, the guy who proposed and named the "Bitcoin Improvement Proposals" if he has an issue with this, or with our BipCot NoGov license. I'm not going to speak for Amir, but I'd willing to bet *Bitcoin to BipCoin* that he thinks the BipCot NoGov license is funny as hell, and a good thing.

"bips" is also what the Bitshares dev team used as virtual "chit" to pay their contractors, and then later cashed out those bips to Bitcoin. I know because I was paid in "bips" when I did work for them.

No chance of confusion there either, that "bip" only has meaning to a handful of people who were paid to work on a system that's not really being developed very much anymore.

"BIP" is a lot of things. Including Bard College's "Bard Information Portal", lol: https://bip.bard.edu/

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 will 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. We will use IPv4 IP for now, but will add IPv6 support later. So the syntax allows will be letters/numbers (and no spaces) up to, let's say 128 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, and from the exchange BipCoin is currently on.

--Or, if easily doable, the much preferable "NON-API ALTERNATIVE" listed earlier in this document, with a long list of all known search engines that return gold price easily.

This should check gold price once a week and should check BipCoin price every eight hours.

--Random number generator
To keep above from overwhelming exchanges with traffic.

--Code to allow domain:IP pair to be added only after payment is made and verified. *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" above in this document for more on that.)

--Code to pay transaction fee of .001 bip to miners.

--Code to pay BipCoin for registrations coming in out to one hard-coded address for Devs and 4 addresses for the four charities. It should have some mechanism to prevent someone compiling our code, and changing those addresses. That is to say, the network must authorize each payment, not a miner.

This addresses could eventually be multisig. But for now, with so many other issues to conquer, it will just be on regular address for the whole dev team, and on address for each of the four charities. (A total of five addresses.)

--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' and charities' websites. This 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. And it won't be a lot of names.

The names will be registered for all time, but IPs can be able to be updated normally, and can be transferred normally to another address if needed.

These existing domains will also be useful to people installing the software, they can use them to test the software to make sure it's working.

With each wallet install, we will include a simple HTML page with a list of our initial Dot-Bip domains and links, so people can test that they've correctly got everything working. Any small images needed for this page will be local in the wallet folder.

CLOSING ARGUMENTS

Distributed DNS is one of the things always mentioned in any introductory article about "the wonders of the blockchain."

Sometimes they even mention Namecoin, or some of the new corporate blockchains. But these articles always act like *it's already a done deal*.

It's not.

They never mention that while this is technically possible, *no one is actually using this yet*. Because no one has solved the main problems and made it easy to use for everyone.

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 did put a car in every carriage house. And when he started most people had never even *seen* a car.

He made cars practical and affordable.

We plan to do this for distributed, difficult-to-censor DNS.

Namecoin established some amazing concepts. But BipCoin will take these ideas and make them easy to adopt for everyone.