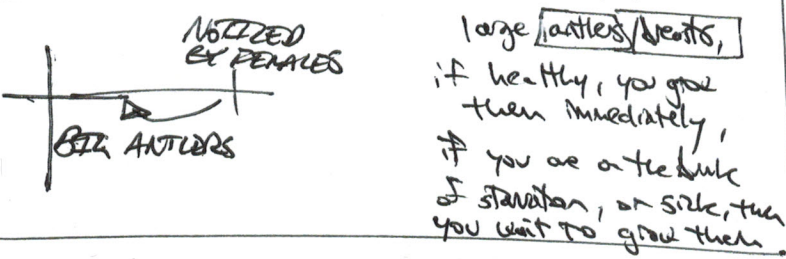
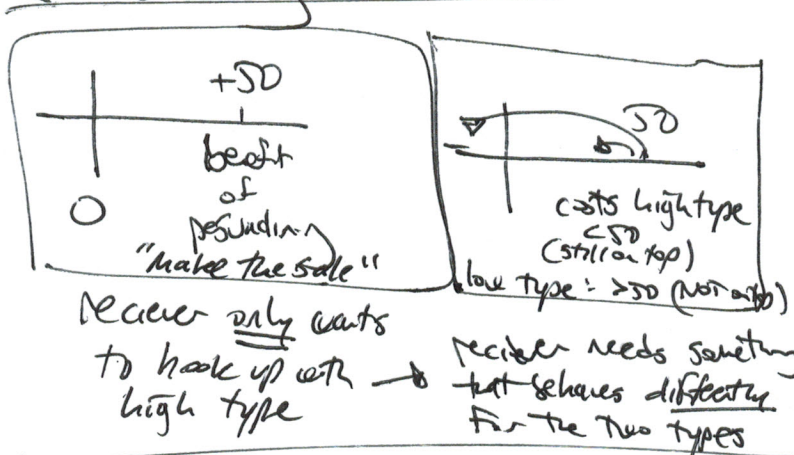


Signaling



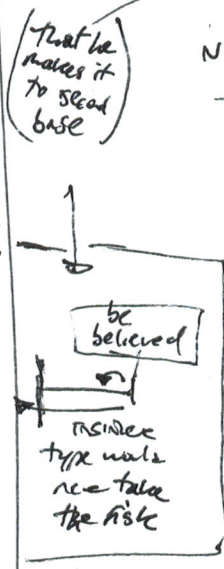
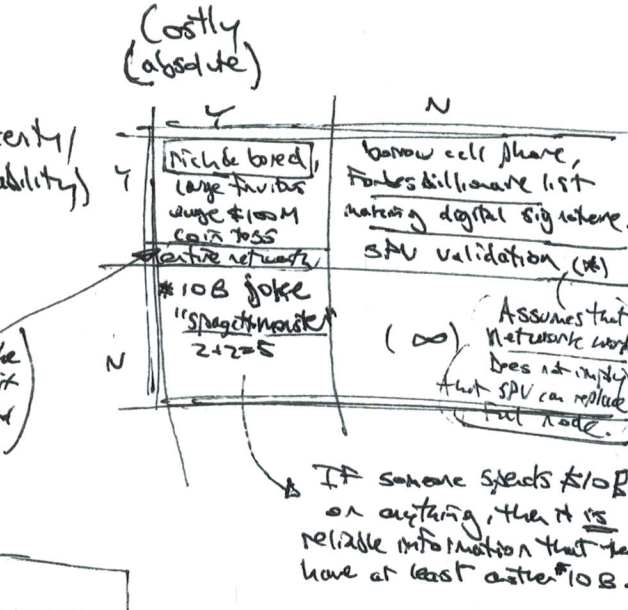
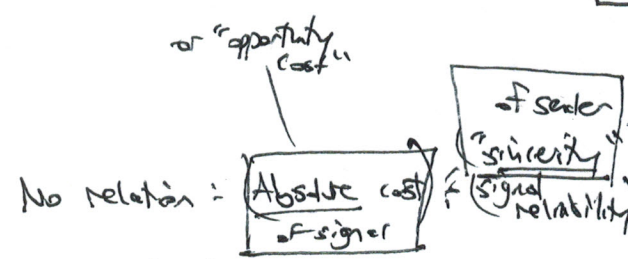
genes/memes, NOT individual selection NOR group selection

gene	memes	(Dawkins)
...next generation • bigger antlers • greater ♀ desire for large antlers • male competition on antler growing	... (C/S/M)... • more pros • greater ♀ pref. for ♂ pretty • makes compete on sending Christmas meme • spreads memes	• doesn't mean gene is good for the animal • meme is true

Megging: not a costly signal
high haspover: NOT a signal → a direct measure of the (seigniorage + tax fees) MR, and the state of hashing tech (hash #).

Waste: The wealthy could buy useful things ~~that~~ that the poor could not afford (eg, a 1st car) (vs no car at all).

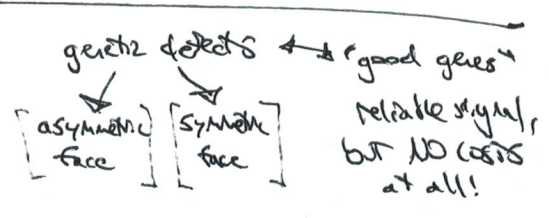
Handicaps optimized to be easily verifiable cost:
 (you could chop off both your arms right now, but it's a high cost)
 • You're talking about handicaps
 • In signaling the absolute cost is irrelevant. In fact if it exceeds the benefit, neither type signals and the scheme falls apart. (can't be > SD)



sincere type would
 sincerity isn't truth, because of the potential for delusion.
 encourages sincere investigation & showing collaboration

Screening:
 • Receiver moves first
 • Sender reacts

(hashpower: any block that meets the criteria, passed or)
 Measures are not signals
 • hashpower has an incredible range and can be measured very specifically, measuring is precise and easy (by-product of computation)
 digital signature verification also precise & easy (cheaper, even more reliable - not less)
 [design of hashpower explicit: no pre-defined public key]
 [peer-to-peer]



Against the Hard Fork

1. Whole point of blockchain is to synchronize everyone's UTxO set. The hard fork de-synchronizes it.

People deciding

2. Big Network Effects

A) Monetary Revolution is extremely disruptive. People's life plans are very dependant on their monetary infrastructure. New monies are very subversive/rebellious.

Drawn for 3rd parties

B) The whole advantage of money (over barter) is that there is just one money.

C) Developers - they must invest a lot of time into learning a codebase. Obviously they prefer to learn a codebase that they think has a future. And a codebase is more likely to have a future if developers are interested in it. Thus completing a circle. New positive feedback loop, new network effect.

D) Similarly, investors might say: "Which of these coins has a future? Well, this one is #1, must be #1 for some reason (EMH). If other investors think like that, coordination problem is solved.

(Aside from ME) Special Advantages to being the status quo AND especially to being #1

status quo

a) The so-called "Live by the fork; die by the fork" problem. Which is to say, when ~~we~~ (if ever) do we stop hardforking and just work together as a team. (EMH -> BSV, Army) As BSV grows, there will be disagreements leading to some people wanting to fork.

b) The fear of miscoordinating. No one wants to find themselves without teammates. ~~And~~ People are afraid of being split up, but for every single unsatisfactory status quo, there are a near infinite number of ways it might be modified. So you are a tiny mote of dust, in an immense sphere of death - if you want to move the mote of dust somewhere, you need to make sure everyone else moves as well. Every group has malcontents, and no location within the sphere will be completely perfect - so safer to just stay with the status quo. "Go along to get along".

In Bitcoin it is worse because the technical complexity of the project make all forms of collaboration difficult. How do you persuade people that lagelocks are ~~better~~? How do you know that they actually have been persuaded for good? How do you even know that you are right??

#1 On top of all of that,

there are special advantages ~~to~~ possessed only by the community that is #1 on coinmarketcap.

It is like all the coins are on a big hill, with a fortress at the very top. And BTC lives there.

D) One advantage is that all the non-#1 coins can be labeled as deviant. And so they can be stigmatized as (being ~~unstable~~ ^{easily disintegrated}, distoyal) likely to fork again. Adherents have proven that they are somewhat wild and untake-able (which might be good for them, but which is bad for winning a war based on network effects). Only

the #1 coin can attract newcomers without stigma.

B) . . .

Mature adults know that when a large number of diverse people are involved you can't do something just because you think it's better. You might be wrong. You might be right but others may not yet believe you, making it contribution.

Hard Forks Pt 2

B)... The greatest advantage of the #1 community, is the ~~the~~ publicly available UT70 set.

Even for coins like Zcash, the open source software has a way of knowing the owner(s) of a given coin; which means that every has a way of knowing.

As a result, any community (Zcash, Monero, Litecoin) can change software (can change tech) as easily as you or I could change clothes. No inherent connection between the tech and the money at all (a position once championed by Dan Travis?)

Why is this an adv. for the #1 coin? Well, the status quo #1 coin, can always react to a usurper by just hard-forking to transform into a copy of it.

HOW TO HARD FORK SUCCESSFULLY

1. Don't leave the trails, without a good plan. (Snowpiper - they leave and freeze to death in like 5 seconds).

2. Minimize the Pain.

- GAFA: keep UT70 sets the same for AS LOW AS POSSIBLE.
- Minimal Code change: (commit - Patchset "the SMB Bitcoin" (with other complementing))

As time goes on, everything will get worse. New people are only onboarded to one the old one. The upstart, becomes an Altcoin.

Mysteries: * Zclassic * Ethereum Mining

But, there is no corresponding advantage to the usurper. After all, if BSV rose to #1 or CMC, it isn't as though BSV would HF to adopt BTC's tech. Totally asymmetric.

Having different tech (# larger blocksize, smart contracts, assets, Turing completeness, etc) can not help in overthrowing the #1 coin. Instead, you need to build a completely different community. But b/c network effects & status quo, will be difficult. Steps to #6, why not #9?

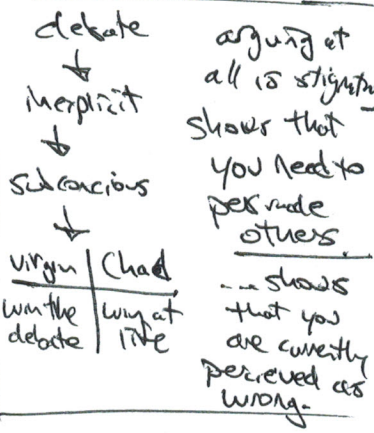
If changed, then the only thing worse would be to change it again.

Definitions of Bitcoin

- shld mean same as they meant yesterday
- can mean different things to different people, as long as that fact is known
- ~~the~~ arguing from definitions ~~has~~ has never persuaded anyone. Definitions are substitutes inside an argument.
- Furthermore, the referent of a word can itself change. So I can say:

In fact, we each speak a private language that only overlaps with others.

Daniel, I was your son originally defined as an infant. But this isn't an infant, therefore it's not your son.



Nash Equilibrium

1. Devs work on #1
 2. Investors only buy the #1 coin
 3. HFs over and over on the #1 coin.
 4. Altcoins are testnets or IMEX.
- IMEX: strategy to stop the #1 community from adopting the reaction-HF (eg. claiming that own tech is best)

BSU

2397 gold	#20	#2000
% 10.17 S&P		

All you have to do is stack up on USD in the SP500 and you are more than compensated for your inflation tax losses.

BSU		BCH		BTC	
Feb 2019 (Tab 6f)	Present	Sept 2017	Jan 2018	Feb 2019	Sept 2020
\$68	\$171	\$444	\$2300	\$726	\$228
+151%		-50%		+81%	

\$367	\$10k
\$15k	
+180%	
+~130%	

If another tribe was better at speaking would you join?

It depends. How much smaller is that tribe? Can my tribe learn how to speak by clicking a merge button or button?

Everybody in BSU wants to win (against other coins).

For now! The underdogs always have an easier time cooperating. As the community grows, there will be conflicts of interest.

You can mistrust (CSW) and think BSU only good.

Why doesn't this apply to Bitcoin? Vladimir?

Other coins have central planners.

What technique do you use, to measure the presence or absence of central planner in a coin.

BSU independent

you look are

May in BSU are conformists.

How do you know that it will?

What if some thought leader thinks that some people shouldn't be able to join?

What if someone joined BSU and said they wanted the blocks lowered?

PROBLEM: Can a good idea get even into Bitcoin if Vladimir hates it?

As long as the answer to that Q is "NO" will always be a tyrant.

What about BCH? What about competition?

Agree

- Cooperation is good
- Competition helps find the best plan (for cooperating on)
- Welcoming people is good.
- Satedan is a user as are many other BTCs, many are active traders, NOT interested in Scholarship/Science/progress.
- Splits are malicious

Not a "meritocracy" Every "ocracy" of every kind that has ever lived, has claimed to be a meritocracy. The true meritocracy NEVER occurs to anyone to bring it up. One day, one giveaway, is that an idea that gets merged, if Vladimir dislikes it.

Advanced COPY vs. Peoples Country

Athen lost to Sparta Rome was sacked by Visigoths 13 colonies vs. British Empire

& their overly adv. is open source software that anyone can steal

one or idea exists, anyone can use it.

Adaptation + Networks Effect

On top of that - we have all of this squared, because people might plausibly think "well, none of this bothers me, but I worry it might bother others". So each of these hurdles is actually two hurdles. Disaster.

(SW)

Creates an "unwelcoming atmosphere"

1. He sues people - should only turn to the State as a last resort - in a frivolous, vindictive way.
2. His unsubstantiated claim to be Satoshi, is offensive to fanatics - the people who work hard to make Bitcoin success.
3. ~~He~~ Gavin and Roger Ver both trusted him, and he stabbed both of them directly in the back, so he's just not a very trustworthy person. Not good associate.
4. Numerous extremely severe allegations of ~~fraud~~ plagiarism, fake degrees, fake ~~websites~~ web pages, fake digital signature, perjury under oath, ~~conning~~ conning people, etc. That drives people away from BSU in ~~many~~ many ways - one is that no one wants to be ~~complicit~~ complicit in any scheme - even unintentionally. The second is any scheme that is ~~malicious~~ malicious.

"People might think I'm a sucker" - which is humiliating. It's the coin for suckers.

Third and most important, why would you give money so someone who might be, a con man. If he coned these other people, a prudent person would ask themselves: How do I know I won't fall under the spell?

Scalability

Money is fundamentally about scale - 5 people trapped on a desert island. They will invent a lot of things - fishing nets, making electricity maybe. But they will never invent money.

Layer 1 - @ 7 tx/sec
(pure onboarding) 220 million per year

34.4 years for 7.6 billion people

↳ LW can't onboard directly. Needs L2 tx

If Bitcoin is to replace banks, will need to do some kind of protocol upgrade (Softfork Fork)

- Layer 1 shouldn't be resource intensive
- Should focus on 100% World's payments, or if we can't achieve that, we should probably go in the opposite direction and reduce the blocksize and make Bitcoin like digital Rare Air of something for ultra-rich people.

- custodial
- Ethereum 83k
32k, 100k LW

Money

Definitions
↓
Properties
↓
Functions

what you need, to buy things
Method of Payment

Money has a convergent yield and speculative value

coin operated laundry machine (you need quarters!)
In Europe, you need Euros. If the restaurant doesn't "take USA" then...

Medium of Exchange

no one would want to hold money, it is just "in between," a conduit

World of infinite liquidity, very easy to change \$100 sticks to \$100 apples or \$100 shoes

Merely a medium, like air & conversation

seller dictatorship

between buyers and sellers
(?) We already use fiat currencies as MoE, so why not?

Silk Road made Bitcoin money, Ransomware etc. Build more things that can pay in BTC, but not in USD.

lower fees & greater adoption

Normally, economists like to look through the veil of money. However, when studying money, we can't do that. We have to look directly at the veil of money.