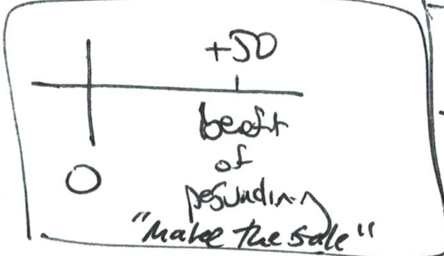
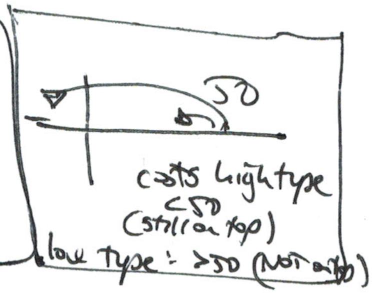
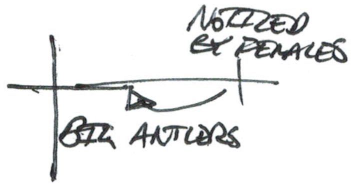
Signalling





receiver only wants to hook up with high type → receiver needs something that behaves differently for the two types



large antlers/breasts, if healthy, you grow them immediately, if you are on the brink of starvation, or sick, then you wait to grow them

genes/memes, NOT individual selection NOR group selection

gene ... next generation	meme ... (FSM) ...
• bigger antlers • greater ♀ desire for large antlers • ♂ male competition on antler growing	• more pious • greater ♀ pref. for ♂ piety • males compete on seeming Christian-like meme [spaghetti memes]

(Dawkins)

• doesn't mean gene is good for the animal
• meme is true

Begging: not a costly signal

high hashpower: NOT a signal → a direct measure of the (seinorage + tx fees) MR, and the state of hashing tech (hash/$).

Waste: The wealthy could buy useful things [redacted] 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, ...

→ • 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.
(...)

or "opportunity cost"

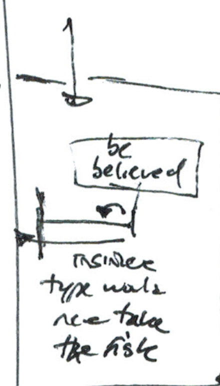
No relation: Absolute cost of signer ≠ (signal reliability) "sincerity" of sender

Costly (absolute)

Sincerity/ (Reliability)	Y	N
Y	Nick be bored, large fountain, large $100M coin toss, entire network, *10B joke "spaghetti monster" 2+2=5	borrow cell phone, Forbes billionaire list, matching digital signature, SPV validation (*)
N		(∞) Assumes that network works. Does not imply that SPV can replace full node.

(That he makes it to Steak base)

→ If someone spends $10B on anything, then it is reliable information that they have at least another $10B



[sincerity isn't truth, because of the potential for delusion.]

betting (encourages sincere investigation & showing collab)

Screening: • Receiver moves first • Sender reacts

((hashpower: any block that meets the criteria, passes etc))

→ 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 predefined public key]
[peer-to-peer]

genetic defects ↔ "good genes"

↓ [asymmetric face] ↓ [symmetric face]

reliable signal, but NO COSTS at all!

Against the Hard Fork

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

(People deciding)

2. Big Network Effects

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

~~B)~~ Incorrect 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.

Hard fork has the potential for failure, SV really does

(Aside from NE)
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 ~~do~~ (if ever) do we stop hardforking and just work together as a team. (~~BCH~~ → BSV, Amaury) 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. ~~People~~ People are afraid of being split off, 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 have the mote of dust somewhere, you need to make sure everyone else moves as well. Every group there 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 communication difficult. How do you persuade people that larger blocks 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 possessed only by the community owning the coin 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.

A) One advantage is that all the non-#1 coins can be labeled as deviant. And so they can be stigmatized as (being ~~untrustworthy~~ disloyal, easily distracted, likely to fork again). Adherents have proven that they are somewhat valid and virtue-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

Hard Forks pt 2

B)... The greatest advatage of the #1 community, is the ~~UTXO set~~ publicly auxiliable UTXO 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 everyone 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 Kravisz!)

HOW TO HARD FORK SUCCESSFULLY

1. Don't leave the trash, without a good plan.
(Slow peeve — they leave and freeze to death is like 5 seconds).
2. Minimize the Pain.
   - HARD: keep UTXO sets the same for ASIC and GPU.
   - Minimal Code Change: I count. Patchset "the 8MB Bitcoin" (weird other complex thing)

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 Dancing

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

Definitions of Bitcoin

- Could mean same as they meant yesterday
- Can mean different things to different people, as long as that fact is known "Bitcoin" "Bitcoin"

(In fact we each speak a private language that only aspires to overlap with others)

- ~~Arguing~~ arguing from definitions ~~has~~ has never persuaded anyone. Definitions are subsets inside an argument.
- Furthermore, the referent of a word can itself change. So I can say:

Daniel, ~~Bitcoin~~ wasn't your son originally defined as an infant. But this isn't an infant, therefore it's not your son. ~~Bitcoin~~

debate → implicit → subtractions → virgin | Chad
virgin: wins the debate
Chad: wins at life

arguing at all is stigmatized shows that you need to persuade others.

...shows that you are currently perceived as wrong.

Nash Equilibrium

1. Devs work on #1
2. Investors only buy the #1 coin
3. Hash over and over on the #1 coin.
4. Attacks are tethered or IMEX.

IMEX: strategy to stop the #1 community from adopting the new (eg. Classic tech)

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.

But, there is no corresponding advantage to the usurper. After all, if BSV rose to #1 on 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 the network effects & status quo, will be difficult.

BSV

	1913	2020
4317 gold	$20	$2000
% $10,127 S&P		

All you have to do is stash your USD in the S&P500 and you are more than compensated for your inflation tax losses.

BSV		BCH				BTC		
Feb 2019 (Twitter)	Present	Sept 2017	Jan 2018	Feb 2019	Sept 2020	$4283	$3647	
$68	$171	$444	$2300	$126	$228	$154	$10	
+151%				+81%			+180%	
			-50%				+1130%	

If another tribe was better at specializing wouldn't you join?

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

Everybody in BSV 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.

What if some thought leaders think that some people should not be able to join?

What if someone joined BSV and said they wanted the blocksize lowered?

Agree

- Cooperation is good
- Competition helps find the best plan (for cooperating on)
- Welcoming people is good.
- Satoshi is a loser as are many other BTCers, many are attention seeking, NOT interested in scholarship science/progress.
- Splits are malicious

You can mistrust CSW and think BSV only good

Why doesn't this apply to Blockstream Wladimir?

PROBLEM:
Can a good idea get ever into Bitcoin if Wladimir hates it?
As long as the answer to that Q is "NO" will always be a tyrant

What about BCH? What about competition?

Other coins have central planners.

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

- Not a "meritocracy" Every "-ocracy" of every kind that has ever lived, has claimed to be a meritocracy. The true meritocracies is NEVER occurs to anyone to bring it up. One due, one giveaway, is that an idea was get merged in Wladimir clo

BSV independent the BSV economy will grow

You Derek are

Many in BSV are conformists.

How do you know that it will?

Advanced country vs. Popular country

Athens lost to Sparta

Rome was sacked by Visigoths

13 colonies vs. British Empire

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

once an idea exists, anyone can use it.

Adoption + Network 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.

CSW

Creates an "unwelcoming atmosphere".

1. He sues people - should only turn to the state as a last resort - in a limited, restrictive way,
2. His unsubstantiated claim to be Satoshi, is offensive to Bitcoiners - the people who work hard to make Bitcoin success.
3. Hal Finney 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. Nor good associate.
4. Numerous extremely severe allegations of plagiarism, fake degrees, fake web pages, fake digital signature, perjury under oath, conning people, etc. That drives people away from BSV in two ways - one is that no one wants to be complicit in any scheme - even ... "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 conman. If he conned these other people, a prudent person would ask themselves: "How do I know I won't

Scability

Money is fundamentally about scale — 5 people trapped on a Desert Island. They will invent a lot of things — fishing nets, roofing, electricity maybe. But they will never invent money.

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

Layer 1 - @7 txn/sec

(pure onboarding) 220 Million per year

34.4 years for 7.6 billion people

LN can't onboard directly. Needs L1 txn

~~If Bitcoin is to Replace~~ banks, will need to do some kind of protocol upgrade (~~soft~~/hard fork)

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

Money

Definitions ⇩ Properties ⇩ Functions

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.

"what you need, to buy things"

Method of Payment	Medium of Exchange
Money has a convenience yield and speculative value	no one would want to hold money, it is just "in between" a conduit
coin operated laundry machine (you need quarters!) In Europe, you need EUROS. If the restaurant doesn't "take VISA" then...	World of infinite liquidity, very easy to change $100 stocks to $100 apples or $100 shoes. Merely a medium, like air & conversation
seller dictatorship	between buyers and sellers
Silk Road made Bitcoin money, Ransomware etc. Build more things that can pay in BTC, but not in USD.	(?) We already use that currencies or MoE, so ~~primary~~ yet. lower fees & greater adoption