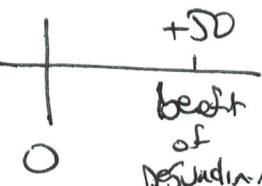
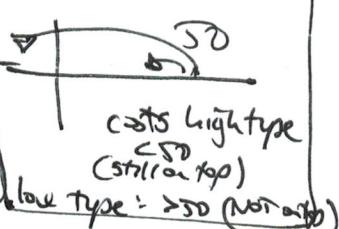


# Signalling



Receiver only wants to hook up with high type



Receiver needs something that behaves differently for the two types

NOTiced by others

big outliers

large outliers/breeds,  
if healthy, you give them immediately,  
if you are at the bank of starvation, or sick, then you wait to give them.

genes/memes, NOT individual selection  
NOR group selection

gene	memes	... next generation ...
- bigger outliers	... (ASW) ...	(Dawkins)
• greater ♀ desire for large outliers	• more pros	• doesn't mean gene is good for the animal
• ♂ male competition in outlier growing	• greater ♀ pref. for ♂ pretty	• here is true

Hegging is not a costly signal

high hashpower: NOT a signal → a direct measure of the (storage + tx fees) MR, and the state of leading tech (hash #).

Waste: The wealthy could buy useful things ~~that the poor could not afford~~ (e.g., 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 the value cost)

→ - You're talking about handicaps  
- In signalling the absolute cost is irrelevant. In fact if it exceeds the benefit, neither type signals and the scheme falls apart.  
(can't be  $\geq SD$ )

No relation: **Absolute cost**  
of sender

"sincerity"  
Signal reliability

(Costly  
(absolute))

Sincerity/  
(Reliability)

N	Y	N
Rich & bored, large fortune large \$100M coin loss entire network	know self above, Fakes billionare list making digital signature.	SPV validation (10B)
*10B joke "Suggermation" $2+2=5$	(∞) Assumes that network works does not imply that SPV can replace full node.	
That he makes it to stand base		IF someone spends \$10B on anything, then it is reliable information that they have at least one \$10B.



richer type would  
not take the risk

sincere type would

sincerity isn't true,  
because of the potential  
for delusion.  
encourages sincere  
investigation &  
showing code

## Screening:

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

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 predicted public key]

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 de-synchronizes it.

## 2. Big Network Effects

A) Monetary revolution is extremely disruptive. People's life plans are very dependent on their monetary infrastructure. New moves are very subversive/rebellious.

~~Involved for 3rd parties~~

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

C) Developers - they must meet a lot of the hits leaving a codebase. Obviously, they prefer to leave 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 poshc 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 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, Armory) 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 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 else, 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. "As along to get along".

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

HTS On top of all of that,

there are special advantages possessed only by the community owning the coin that is #1 in 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 ~~wasteful~~, ~~distributed~~, ~~jeopardized~~, ~~likely to fork again~~).

Adherents have proven that they are somewhat wild and untameable (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 mature 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 coercion.

# (Hard Forks pt2)

B)... The greatest advantage of the #1 community is the ~~privilege~~ publicly available UTxO set. Even for coins like Zcash, the open source software has a key attacking the owner(s) of a given coin; which means that everyone has a key attacking. 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 Travers!)

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 trail, without a good plan.  
(Slow person - they leave and freeze to death is like 5 seconds).

### 2. Minimize the Pain.

- GAP: keeps UTxO sets the same for Altcoins.
- Mitred Code Change: (commt. Patchset)  
"the SMB Bitcon" (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 Darling

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

• In fact,  
we each  
speak a pure  
language that  
only aspires to  
overlap with  
others

• Can mean different  
things to different  
people, as long  
as that fact is  
known "q"

• ~~arguing from~~  
definitions ~~has never~~  
persuaded anyone. Definitions  
are substrates  
inside an argument

• Furthermore, the  
referent of a word  
can itself change.  
So I can say:

Daniel, ~~wasn't~~ your  
son originally defined  
as an infant. But  
this is MATT on what  
Therefore it's not  
your son. "

debate  
+  
Meriticit  
+  
Succinctness  
+

Virgin | Chad  
win the debate | win at life

arguing at  
all is ~~stagnant~~  
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. HFs over and over on the #1 coin.
4. Altcoins are testnets or IMEX.

IMEX: strategy to stop the #2 community from adopting the reaction-HF (e.g. claiming that our own tech is bad)

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 have 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 before Network effects &  
status quo, will be difficult.

Step to #6, play not #9?

BSV

16397 gold	\$20	\$2000
% 210,177 S&P		

All you have to do is  
stash your USD in the S&P 500  
and you are more than  
compensated for ~~the~~ your  
inflation tax losses.

If another  
tribe was  
better at spending,  
would 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.

You can  
mistrust (SW)  
and think  
BSV only good

Why doesn't  
this apply  
to Blockstream  
WebMoney?

Other coins  
have central  
planners.

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

BSV  
independent  
the BSV  
economy will grow

You  
Delek  
are  
Many in BSV  
are conformists.

How do you know  
that it will?

(SW)

Creates an "unwelcoming atmosphere".

1. He sues people - should only turn to the state as a last resort - in a ~~judicial~~ ~~judicative~~ way,
2. His unsubstantiated claim to be Satoshi, is offensive to ~~factories~~ - the people who work hard to make Bitcoin succeed.
3. ~~He~~ Jason Grinn and Roger Ver both trusted him, and he stabbed both of them directly in the back, ~~so~~ so he's just not a very trustworthy person. Nor good associate.
4. Numerous extremely severe allegations of ~~he~~ plagiarism, false degrees, false ~~websites~~ web pages, false digital signature, perjury under oath, ~~he~~ conning people, etc. That drives people away from BSV in ~~these~~ ways - one is that not one wants to be ~~compliant~~ in any sphere - even unintentionally. The second is that no one wants to be ~~compliant~~ with the malicious.

BSV

Feb 2019 Present  
(Tweets)

\$68 \$171  
+ 151%

BCH

Sept 2017 Jan 2018 Feb 2019 Sept 2020  
\$4283 \$3643  
\$15k \$10k

\$444 \$2300 \$126 \$228  
+ 81%  
- 50%  
+ ~130%

22

\$3643  
\$10k  
+ 180%  
+ ~130%

Agree

- Cooperation is good
- Competition helps find the best plan (for cooperating on)
- Welcoming people is good.

Safedean is a loser  
as are many other BSCers,  
they are anti-intellectual,  
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  
meritocracies at NEET  
occurs to anyone to  
bring it up. One  
due, one giveaway,  
it's that an idea that gets  
helped, it WebMoney dislikes

Advanced  
Country  
vs.  
Poor Country

Athenians lost  
to Sparta

Poleis were  
Sacked by  
Visigoths  
13 colonies vs.  
British Empire

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

one or  
idea  
exists,  
anyone  
can use  
it.

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.

Adoption +  
Network  
Effect

- "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 to someone who  
might be a con man.  
If we could trust these other  
people, a prudent person  
would ask themselves:  
How do I know I haven't  
fallen 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, boating, 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

LN can onboard directly.  
Needs L2 tx

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

- 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 art or something for ultra-rich people.

- custodial
- Ethereum 83k  
32x, 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

Money has a convenience yield and speculative value

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

Seller dictatorship

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

## 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 stocks to \$100 or \$100 shoes

Merely a medium, like a M&M conversion between buyers and sellers

(?) We already use fiat currencies as M&E, so why money yet?

lower fees & greater adoption