Phases of a Crypto Bull Market

Abstract

Bitcoin is here to stay because due to its use as a hedge against inflation and for off-shore banking. Bitcoin doesn't compete against other cryptos with features, rather its inefficiency and unchanging code is its core value proposition. When trading Bitcoin, make sure to be broad and not get blown up with a few risky trades. Keep an eye out for the future of cryptocurrency with regards to interoperability and DeFi.

1 Bitcoin Bull Theses

Advice: When events should kill and asset but don't, take notice. In 2014, everything went wrong for Bitcoin. Silk-road, which was Bitcoin's biggest usecase was taken down and Mt. Gox and subsequent crashes. But Bitcoin did not die out.

Info: Off-shore banking analogy: a $20-30 trillion market. Billionaires and S&P500 companies all have assets spread out with many bank accounts, such that if ever some of their bank accounts get frozen due to unexpected court showings, etc, they can still remain solvent. Bitcoin is a perfect alternative off-shore banking system where assets cannot be arbitrarily frozen or seized.

Info: Obvious adoption curves. People learning about Bitcoin mostly ended up becoming a believer. Smart people are getting in and buying.

Info: Dollar depreciation. Fixed emission curve. Tested social concensus. Hard-forks were attempted and failed.

2 Bitcoin and Cryptocurrency Fundamentals

Fact: Huge friction to adopt new technology, no new technology will be adopted due to 2% in savings. Bitcoin does not make sense as a payment rail (will never replace VISA).

dvice: Treat Bitcoin like an option. Bitcoin is an asset that routinely falls 80%. Expect that sometime in the future, this asset will fall 80%.

Info: Bitcoin has boom-bust cycles and intrinsic value is network driven. For example, the more people accept Bitcoin, the more liquid it becomes and thus the more value it's worth.

Info: Bitcoin doesn't compare on features. Most new technology competes on technology, ie features, efficiency, etc. Early first leaders are often leap-frogged because there is so much innovation happening and it's not about that first patent or breakthrough, but rather the 10th patent, etc. Exception is Bitcoin. Bitcoin is comparable to JP Morgan. JP Morgan gets found guilty of money laundering, drug trafficing, etc, every year and gets fined, but they are not going to get shut down because of their size. Similarly, JP Morgan doesn't worry when a new bank offers 5% less fees because JP Morgan is not competing on the features but rather on the fundamentals tied to their longevity. Bitcoin's moat: Anonomous creater and relatively unchanged code that has survived for a decade.

Info: Core value proposition: it makes no sense trying to optimize Bitcoin as a payment rail beacuse Bitcoin is a terrible payment rail. There are many other projects that do much better. Bitcoin's core value stems from that it's optimized and obselete technology is stable at the protocol, code, and governance levels.

Reasoning: Bitcoin is perfect as a use for collateral except for its volatility, which will decrease with time via increased adoption.

Theory: Bitcoin network may be most secure settlement layer. One example making Bitcoin network more secure than SWIFT is that US cannot arbitrarily cut countries off the network (North Korea, Iran). In 5 or 10 years, companies will be settling their transactions (not necessarily in BTC) on the Bitcoin network.

Info: Entire crypto-currency sector follows Metcalfe's law (value of an asset is equal to n^2 for n users)

3 Investment Advice

Advice: VC mindset was incredibly helpful. You make an investment for 10 years and ignore all short-term volatility.

Advice: Don't blow up. If you have leverage, make sure to not get liquidated and taken out of the game. What is the amount of risk you're taking and the possible reward?

Prediction: BTC is the public crypto store-of-value pay. BTC blockchain is the most secure settlement layer. Some proof of stake networks that target a niche (federalism) for gaming, speed of transactions, etc will also be successful.

Beware: Don't run into faulty logic using Metcalfe's law. For example, if token X's sector is valued at $1 trillion and token Y is just launched and is competing in that sector, it is faulty logic to say that if token Y addresses 1% of that sector, it will be worth $10 billion.

Advice: Be broad and not concentrated.

Info: In the last portion of the bull-run, alt-coins outperform Bitcoin. Reasoning: People's risk-tolerance grows and have generated their 5x and are looking for their next 5x. Last phase of a bull-run is when the worst coins rising.

Advice: Have basket of high-quality alt-coins, basket of medium quality alt-coins, and basket of shitcoins. This is a short-term (4 months) bet that those assets will rise, not as a long-term play.

Opinion: Of the top 100 coins by market-cap, 70-80 are

fundamentally worthless. Note that if there is a fundamental flaw in the project initially, that does not mean it cannot be fixed. Make sure to look at the competence of the team and practiability of the vision.

Advice: Do not hold 100 crypto assets, 20 is good enough (based on removing 80%)

Advice: Learn how to value cryptos. ie, what's the percentage of a hardfork on crypto X and the value of the forks, etc, requires deep technical understanding and what technical information matters. ie, what game-theory exploits exist in a defi launch.

4 Future Innovative Sectors

4.1 Interoperability across blockchains

Atomic swaps: Cryptographic signature on two blockchains that without intermediairy allows transfers of value between blockchains.

4.1.1 Layer 0

Definition: Hold and coordinate communication between layer one blockchains. Meant as an ultimate settlement layer.

Polkadot, which will allow interoperability across many layer ones.

4.1.2 Layer 1

Definition: The blockchain that supports the transactions and communication of a given currency.

Ethereum and Bitcoin are layer one.

4.1.3 Theories

Theory: Bitcoin will be the ultimate collateral layer. Faster transactions with Bitcoin will exist on more efficient blockchains.

Theory: In a world where features are not the diffrentiator (ie for privacy, can use Bitcoin on Monero blockchain, etc), there are only a few instances where Bitcoin cannot be used as the main currency of that blockchain. (1) Monetary policy. Ie, community wanting an asset with a different inflation policy than Bitcoin. (2) Regulatory status. At somepoint someone will launch a blockchain that cannot be atomic-swapped and cannot be made anonomous.

4.2 Defi

Advice: Treat DeFi as hyper-speculative. May make sense to be a staker or provide liquidity if getting 40% return, not for a 4% yield because of multiple previous hacks.

5 Miscallaneous and Further Research

Info: Bitcoin as a solution to custody and rehypothecation

Beware: Hard forks define the minority chain to be unstable. Via game theory, attacks on minority chains that use the same consensus mechanisms as the main chain can be carried out without sacrifice of material as mining equitment can still be used to mine on the main chain.

Question: What are the limits of interoperability?

Fun fact: Hard for hedge-funds to hold crypto and multiple security risks that are not part of their business model exists if they work in crypto. ie, what are the chances someone will do a $5 wrench attack?