~opening~

~cultural tech~

The prediction market is a civilizational technology comparable to the internet, or the prining press … or indeed, Satoshi's blockchain.

The prediction market idea … is SO good, that whenever it springs up, naturally in the wild, it starts causing problems… for all of the horribly corrupt people out there. Who then censor it.

Thus, it's the perfect marriage: Bitcoin would keep these Markets alive, via the immortal blockchain; and these markets are a use-case for Bitcoin. People would buy Bitcoin, just to participate. It would make Bitcoin even more culturally relevant, in a whole new way.

~cultural tech 2~

What makes prediction markets so great?

What *previous* technologies did, with information, was "save it, and spread it" – you know, it preserve information, duplicate it, and ship it out to people – distribute it, quickly …

What the blockchain does is *sort and immortalize it* – the proof of work , means that only some of the blessed information rises to the top – of being on everyone's node. And mining, sorts the information by time (solving the double spend problem). And so we all agree on the history.

What the *prediction market* does, is.. *unite* the information. The prediction market *combines* all the knowledge out there –on a given question—into one [[finger]] number. It has the power to make people agree, on questions. You get one number, that is the *same for everyone*… Such that if anyone disagrees with the number – president, CEO, prime minister, academic, military general -- if *anyone* disagrees with it, they can be safely *ignored.* Or even made fun of. It makes it laughable to oppose the number. It also scales in a completely different way – ordinarily more information sources just means more complexity, more noise. But prediction markets, more people means more liquidity – more accuracy. More persuasiveness.

And that makes it NEW. It's very underappreciated.

So I look forward to explaining it.

~Agenda~

Here's the agenda. Introduction of myself. What are prediction markets. Then – the very special type of "advice giving" multidimensional prediction market. Very important. Finally, I'll talk very briefly on how to do all of this on Bitcoin. Mostly, I'll point you to which websites to go to, to do your own research, if you're interested.

~About me~

Ok -- I joined the Bitcoin community in 2012. At that time -- I was working at the Yale University Economics Department. I wrote some code in 2013, and a paper in Jan 2014 --kind of a long paper—on “Bitcoin Prediction Markets”, this talk. That paper was called “truthcoin” – which is very unfortunate because, back then, that was so early, that there really were no altcoins. (there were like a few) Like Namecoin – see namecoin was a real project though. So you know – having “something”-coin , it was a bitcoin project. Anyway, I then renamed it to “Bitcoin Hivemind . com” . So that’s the site to visit – Bitcoin Hive-Mind .com that site will tell you all you need to know, and more. And you can even see the old software – we are now rewriting it in rust. Here in this tiny little talk, I’m just going to give a small overview.

~my 1000 pages~

After I renamed the project to “BitcoinHivemind”, I turned Truthcoin.info, into a Bitcoin blog, where I’ve written over 1,000 pages of deep commentary on technical Bitcoin issues.

~my big break~

My big break – so to speak – was in Dec 2014, when Adam Back linked to my blog. I wrote a famous essay called “Nothing is Cheaper Than Proof of Work” which was a very early critique of Proof-of-stake. Then I sort of became a little more famous.

~since then~

Since then, I often speak at Bitcoin Conferences -- especially the technical ones such as TabConf. And I go on podcasts.

I’m best known today – and we have to get this out of the way – for being the creator of “drivechain” – which is BIPs 300/301.

Drivechain is a much better idea that this one here, today. Its practically inevitable, its almost guaranteed to work, its much simpler. So if you want something rock solid, go with that – this, in this presentation, is more of a high-risk high-reward type idea.

Drivechain gives us L2s with planetary scale, and L2s with zCash privacy. It also gives miners hundreds of Billion Billions of dollars of extra revenue per year, and a whole bunch of other things. Its 10 years old now, and people are slowly realizing that it is the only way for Bitcoin to succeed.

~screenshot~ [[6: 20]]

But don’t take my word for it – try it yourself, go to LayerTwoLabs.com/download . LayerTwo Labs is my company. We have a scale sidechain, zCash sidechain – a clone of the zCash altcoin (but with Bitcoin only, no z-coin), and a clone of Ethereum. And whole lot else. So try it for yourself – a lot of people are *really confused* about the Drivechain project. Plenty of people lie about Drivechain -- because they are afraid of how good it is. (In that way its very similar to prediction markets.) But if you just try it yourself, you’ll see that everything else in Bitcoin is a .. big waste of time. I’ve already solved all those problems, scale, mining decentralization, fraud proofs etc, and now I’m moving on to the next big thing… which is this…

… these prediction markets.

~math~

Ok, so – prediction markets make everyone an expert.

So, here's a math question… in the top right…and here are some responses, maybe…

~math + midwit~

Now, with prediction markets, everyone is an expert. Even the little guy – someone is not very smart, OR someone who is easily tricked, OR just someone who ***hasn't had time*** to look into it (I mean, we can't look into everything).

~grug + with PM~

… they'll all be able to see, the prediction market's answer, all day every day. – because the answer takes the form of a market price – it s a public number, that everyone see and everyone can trade against. Smart money.

~bubbles~

The market is betting that the answer is near 126. They're putting money on it, it must be right. Not necessarily, but probably. I mean – why destroy your own money?

~controversial questions~

Now – the math question example, has the property that it is ***not controversial***. Before its solved, no one knows. After it's solved, everyone agrees. So the unification property of prediction markets, isn't very useful.

But what about ***these*** questions?

These are things people disagree about.

I have one example for you.

~Intrade Global Warming Example~ [[9 : 00]]

This is an example from intrade. This is a real world prediction market. Or at least it was. This asset was created in 2011, and the issuer – a company called INTRADE -- would've bought it back from you, for one dollar, if the year 2012 had been the warmest year on record, as reported by these NASA satellites that measure surface temperature (and report it ***after*** the fact)… NASA puts this on a website… where anyone can find it. Otherwise, the asset is worth zero.

The future is hard to predict. The answer isn't totally clear on day 1. So, in real life, this asset traded at 40 cents in Jan 2011 but by mid-2012 it was worth just ten cents, and in Dec 2012 it was worth nothing.

So, a prediction market is similar to a “bet” or “wager”. But the difference is… a constantly changing price , that anyone can contest. In a bet, the odds are fixed; usually my $100 against your $100. The winner keeps $200. But that’s pretty lame, really. That’s very clunky. Instead -- with these assets, the market price changes all the time – and its current value is the objective likelihood of the event in question. As 2012 went on, it became clear that it wouldn’t be the warmest year, so the price collapsed. You could watch it change every day.

(And if you knew, all along – in January – that it wouldn’t happen, then you could have made money. Because there was a parallel “NO” contract that traded at 60 cents and went up to 100 cents. Either way, you buy low, sell high. If you want to critique the market, it must take the form of a trade *in* the market.)

So that’s the prediction market: an asset that pays you money if something happens. If it happens, you get paid. If it doesn’t happen, you don’t. Anyone in the world, can buy or sell.

~circle bottom two questions~ [[11: 20]]

Now I have to apologize – I’m now going to focus on this one Trump example. It’s just better to stick with one example, all the way through. – I assume you’ve heard of Trump. It’s an example for the whole world.

I’m sticking with this one example, BUT that is very unfair and misleading to you. This idea, can be applied, whenever we want *lots of people* all to become *very smart* on a *controversial* topic.

But I’m going to narrow it to this Trump topic, for most of the talk.

First, the first of the two: Will trump win. – Not “should”, only “will”.

Everyone’s got an opinion on this question. Everyone has a hunch. And some people are specialists, such Nate Silver – he uses *statistical models*, polling data – the pollsters. Some people are older-and-wiser, and some people are young-and-naïve. It goes on and on – economic forecasts, such as stock market, unemployment rate; geopolical events such as *wars*. Climate change, whatever. So people disagree. Enormously, on the WILL question. How likely is he to win.

But this is where the prediction market will work its magic, and force everyone to have only one answer. There’s only one market price on every given day, and if the price is wrong – buy low, sell high, you make money.

~BetFair~ [[13:05]]

This is real data from the UK site BetFair. The question is: who will win the republican nomination, back in 2016. This is real data from 2016. Trump is in blue. It goes from January 2016 to March 2016.

These are assets that pay out if their candidate wins the 2016 republican presidential nomination. So you just divide, current_market_price / what BetFair will pay you, if it happens. You get a percentage. That percentage, is equal to the likelihood. After the Iowa straw poll,

Trump's market price plummeted. See the blue line going down? Then it surged after he won South Carolina. Goes back up.

Now, thoughout this time, people disagreed. But there was only one prediction market number, for everyone. Publicly available numbers -- everyone can see them every moment of every day. They're just hanging there, in reality.

Is this what I came here to talk about ?

~No~

No. This… … is lame. At best, it is a little entertaing. It's not revolutionary. It only tells us *who* is going to win. If we know someone is a bad candidate, we can't stop them from winning. We just have to sit there and watch as the Titanic crashes into the iceberg, and sinks.

~question slide again~

Instead, we want to predict that the ship will hit the iceberg, and then ***do something*** to fix that. And ***that*** is a completely different type of thing. I wouldn't have flown all the way here, to Hong Kong, to present on the first thing. The first thing, is not that good – but the second thing is revolutionary.

So how do we do it?

~values~

Well, first ingredient -- we predict how well we are currently going to do – with more prediction markets. We create markets on these questions. What will the unemployment rate be? Et cetera. The prediction market will tell us.

Trump, 55% likely to win. Unemployment rate, likely to be 15%. Oh no -- that's very high – that's the iceberg.

But we still have the same problem as before. Are we hitting the iceberg because trumps number is so high, 55 ? He's going to win and screw everything up. Or are we hitting it ***despite*** the fact that Trump's number is 55 ? If only Trump traded at a higher value, then we'd be saved – and future unemployment would be lower. Or? – are they unrelated.

Well, a special type of prediction market can answer this question: the multidimensional prediction market.

It gives ***not only*** the likelihood of each event, (like will it happen or not) but it also gives ***the relationships*** between events.

How? How is that possible?

Well I'll show you. It's actually pretty easy.

~Nine slides~ [[16: 30]]

I will now try to explain it in exactly nine slides. Don't worry, I've done this before. The first two slides are really easy, and four of them are really just one slide, broken into four pieces. I'll summarize it at the end.

~mv1~

Here, on the left I have a series of coin-flip events. In this table, we're describing the behavior of the three-hundred-and-third coin flip. We don't know what will happen on that flip, but we can nonetheless fill in the probabilities in this table. Heads and Tails are equally likely so its 50-50.

~mv2~

Now, this slide is the same as the previous one. But it has a dice roll instead of a coin toss.
Each side of the dice is equally likely to come up, each has one-sixth probability.

~mv3~

Now here we go, three of seven…
This example, is the previous two examples, smushed together.
We have the coin flip in green along the left vertical edge of the table. We have the dice roll across the top horizonal edge.
I've circled some probabilities in red. The probability that two will be rolled, is one-sixth. The probably that a tail will be flipped, is one-half. Those are called marginal probabilities because they're written in the margin, so to speak.
The probability that BOTH a two will be rolled, and a tail will be flipped, is shown here as one-twelfth.

~mv4~
Now, we'll talk about relationships among events. Let me draw a contrast between these two blue tables here.
Both are about unknown future coin flips. The top table considers coinflip three-zero-four, in blue across the top. And it considers flip number three-ohh-five, in red across the left side.
Each cell will occur with probability point two five, which is what I have indicated here.
The second table does something extremely unrealistic, and only useful for teaching purposes. It plots coin-flip #304 against itself.
Again, in the real world, this would never happen. But, if it did happen, what probabilities would we write in this table?

~mv5~

Here's the answer. Fifty zero zero fifty.
Coin flip #304, can either be heads or tails. But it has to be one or the other. So we zero out everything that's impossible.

~mv6~

Here's this example again, with dice instead of coins. Same dice roll, we don't know what it is yet.

~mv7~ [[20: 00]]

But we know that lots of these values are logically impossible. So, when events are related, there's this kind of "clumping effect".

~mv8~

So, since clumping = relatedness. All we do is measure these two things at once. And we look for the clumping. If there's clumping then the events are related.

~mv9~

So, to achieve what I wanted to achieve before -- we just make four separate single-dimensional markets. We get the market price for each, and then look for clumping.

(We don't actually do that – we can do all 4 markets in one, in a much cleverer way that amplifies the liquidity enormously – but I don't have time to explain that right now.)

~Arithmetic~

…we can just add and then divide, to make the clumping explicit. So laypeople will never have to see anything complex.

And that is how you get these numbers to show up.

And you'd see something like this.

Which would eventually translate to…

~example ballot info~ [[22: 00]]

…something like this. For the two candidates, it gives forecasts of how life will be, if they're elected. The first row guesses how much the government will cost, the second row guesses how economically prosperous the citizens will be, and the third row would cover things like, invasion, healthcare, mental health, gun safety etc.

You could even subtract, to make it even simpler.

~menu~

It would eventually look like this. A kind of menu. Just a list of exactly what to expect, for whoever you pick.

~other questions~

Now I have to stress again, that it is a mistake, to focus on my one Trump example. So here are other questions we could re-use that strategy on. [[[read]]].

Now I'm kind of joking with this one, but believe it or not, there were prediction markets back in 2017, on the SegWit2x hardfork. And the prices were split 85% 15% most of the time, and when BCH actually emerged in Nov, it ended up trading pretty close to 85-15. For a while.

In general, this idea works better for the Big Questions – because theres more people, more disagreement, more trading, more information united into the one number.

~triangle~ [[24:00]]

So I have a little image here. Most of life is very tidily organized in a pyramid. You have a boss, it mostly works. But who fires the Top Guy?

~2nd triangle~

See, within the pyramid, things are pretty rational. Your boss observes your work, they get rid of you if you do a bad job. But at the top, it is difficult for a large group of people to Monitor the top guy and coordinate to Get Rid of him. But that's actually what these prediction markets are good at.

Ok --- what about Bitcoin though.

~What about Bitcoin~

Well, its Bitcoin L2 season. It is possible to build a Bitcoin L2 that does this whole thing – create markets, trade, whatever – without talking to any humans. Just from the privacy of your own computer. Private transactions, making money if the price is wrong, OR just viewing the prices. Transaction fees going to the miners.

Now – I don't have enough time to explain all this – but go to Bitcoin Hivemind .com for more information about this project, and my plans.

I do have some screenshots for you, though..

~screenshots~

.. these are old QT version. We're rewriting it now in rust …

~screenshots~

And of course – if it succeeds – if this idea takes off, (or a similar idea) then people all around the world, will turn to *this Bitcoin L2* for answers to all of life's important questions.

~final slide~

Please go to BitcoinHivemind .com , join the DC telegram t.me/DcInsiders to talk to me. I'm @truthcoin on twitter . So, thank you very much.

Ok please come up to me and ask me any questions you might have. Thanks!