Financial surveillance

Regulatory bullshit – bothering normal crypto users while they are buying / selling / using

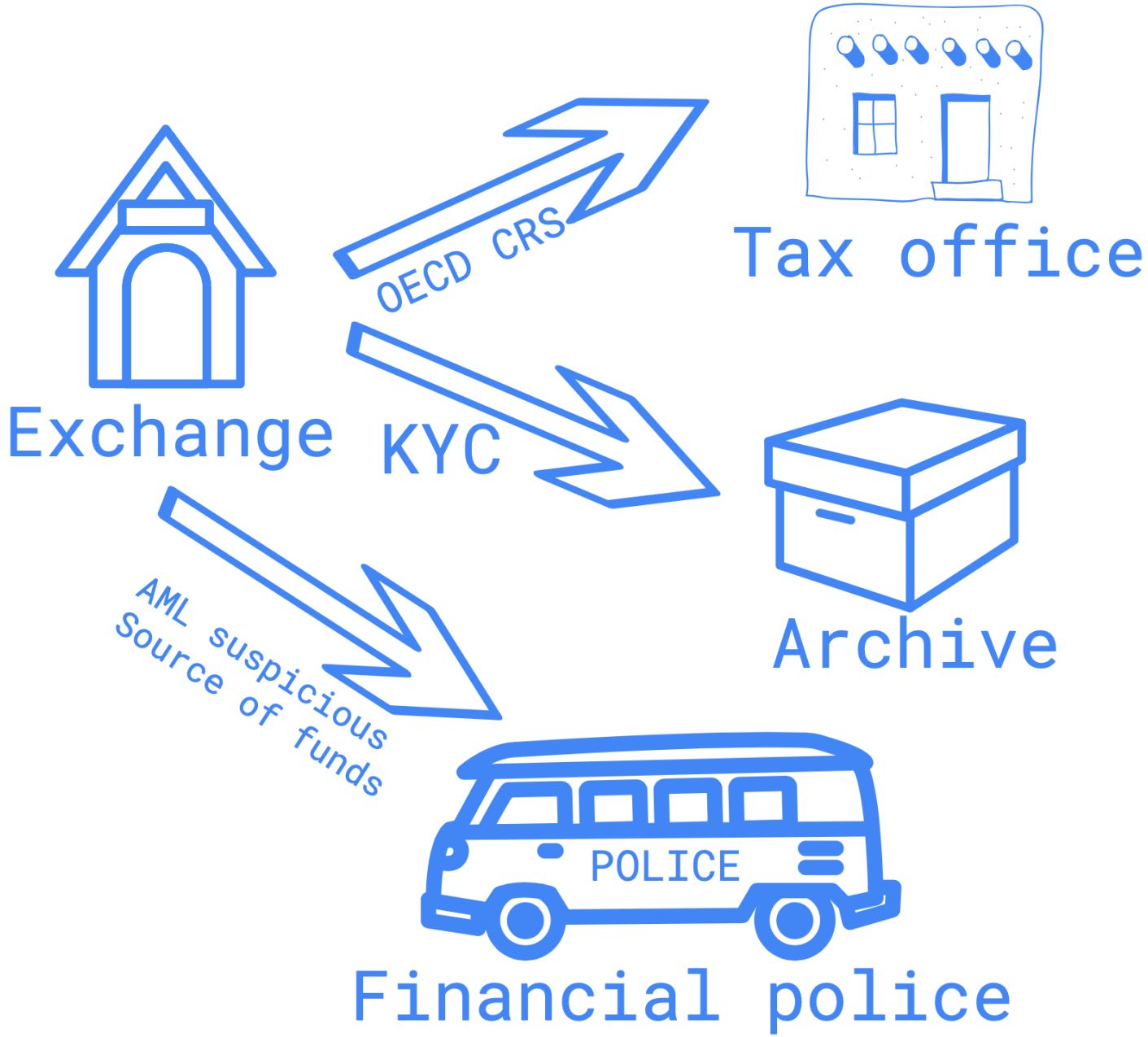
KYC, AML, tax reporting

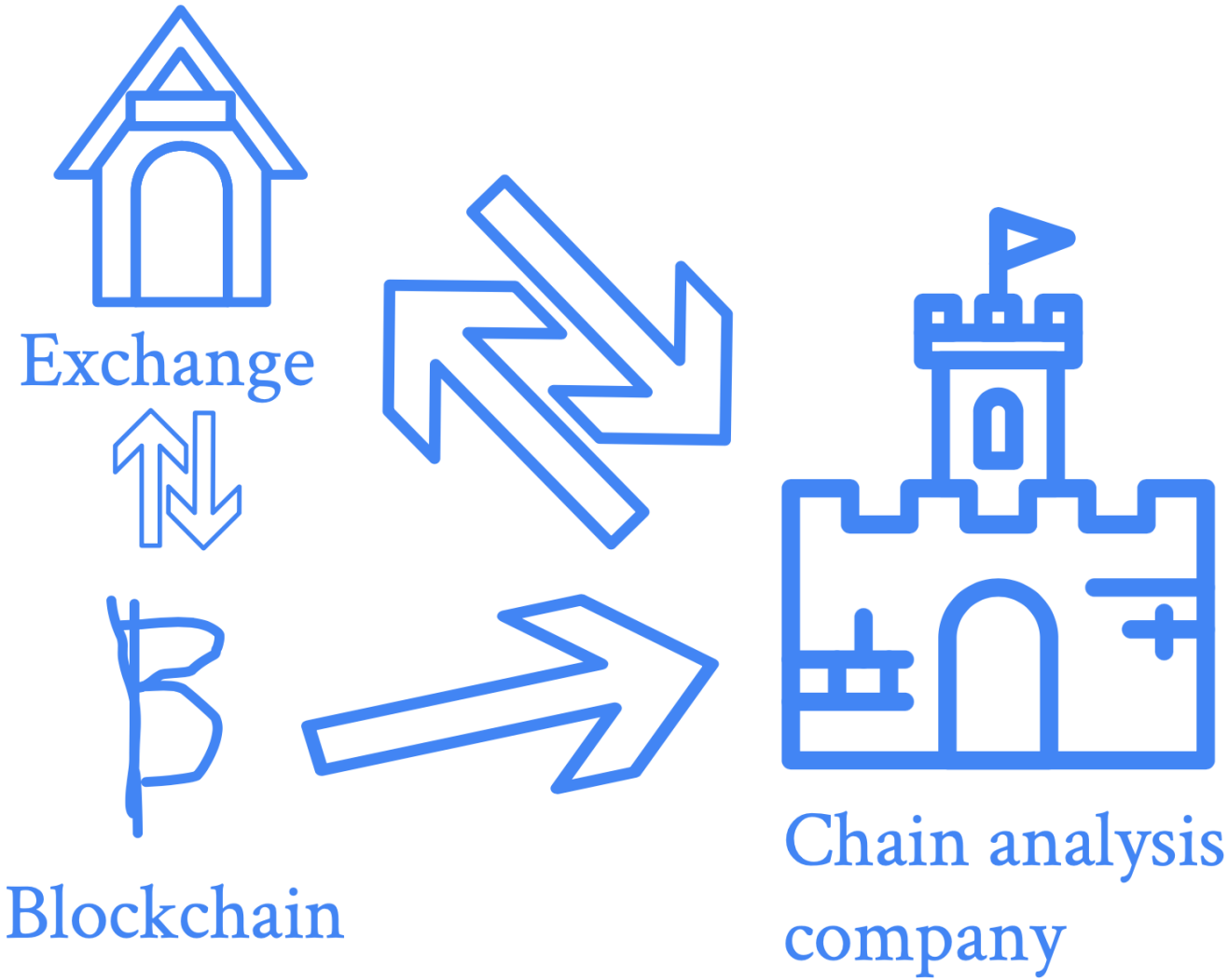
Not only on transparent blockchains – surveillance is much wider problem

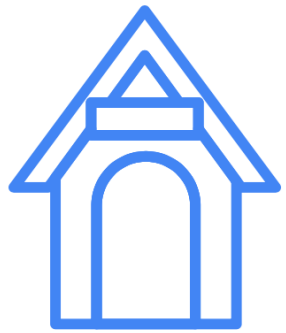
Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.


Exchange
OECD CRS
Tax office
KYC
Archive
AML suspicious
Source of funds
POLICE
Financial police


Exchange
Blockchain
Chain analysis company



Exchange

- OECD CRS
- KYC
- AML susp. transactions and source of funds
- Risk of account closure

Bank

- OECD CRS
- KYC
- AML susp. transactions and source of funds
- Risk of account closure

Regulation of VASPs, etc.

FATF-GAFI and EU want to regulate VASPs and anonymous use of cryptocurrencies

VASP - Virtual Asset Service Provider

- Formerly exchanges, payment gateways, ATMs
- Later, providers of hosted (custodial) wallets
- An effort to expand to payment gateways and anyone who accepts cryptocurrencies or provides this service to third parties (terminal operator, ...)

FATF-GAFI prefers a "risk based approach"

- Non-custodial wallets, anonymous cryptocurrencies, transactions without "travel rule information" are automatically "high risk"
  - => Report the transaction to the financial police, block it, …

What <u>if</u> (when?) such regulations are put into practice?

Proxy merchants

- Direct purchase of goods and services
- Purchase gift certificates

The Veksláks – decentralized P2P exchangers

- They exchange between fiat and crypto

Escape to other countries

- I don't personally prefer this approach, but some have a more favourable environment or are slower to introduce regulations

Cryptocurrencies are a “gateway drug”, not only to parallel financial system, but to liberty. If people choose a private way of acquiring it, they are not choosing only speculation, but other values as well - decentralization, privacy, sovereignty

Inspiration: pot dealers

- Peer to peer despite a highly regulated environment
- High availability anywhere (cities, villages)
- Addresses the problem of regulation
- They provide education
- They have handled security
- Scales well

Vekslák – crypto dealer

Vekslák is part of the market structure of the peer to peer economy

Problems solved by veksláks:

- Balancing supply and demand, even at times when one side dominates
- Privacy
- Education
- Regulations

How to find a crypto dealer?

Localbitcoins (introduced by KYC), localmonero, ...

Is that a good idea? How do you find a pot dealer?

Crypto vekslák groups

- Start it within a group of friends and peers in your city
- Signal, Threema, Element (Telegram is a spyware!)
- “I am buying”, “I am selling” in the trading group
- If you are active in more than one city, become a member of more than one group
- By invitation, by acquaintance, apparent and verified reputation
- Don't be afraid to offer premium/discount
- Discussions in a parallel groups are important
- Don't be afraid to create a parallel economy and trade other things than fiat for crypto
- Some participants may turn into semi-professional veksláks - embrace it!

- https://juraj.bednar.io/cryptotradinggroup

Two sides

FEDERAL RESERVE NOTE
AB 39048518 L
B2
THIS NOTE IS LEGAL TENDER
FOR ALL DEBTS, PUBLIC AND PRIVATE
Treasurer of the United States.
SERIES
1996
100

KB 33366506 F
100
ONE HUNDRED DOLLARS

Exchange rate hedging: Crypto-dollars to paper dollars

- When - The exchange rate has crashed, everyone wants to buy, no one wants to sell. Crypto ATMs don't have crypto. It's hard to do one side.
- Thanks to hedging, we can be a counterparty even in a very unbalanced market
    - …and do the trade no one wants to do
- It's symmetrical, we can do the opposite operation when the exchange rate goes up and everyone wants to sell.

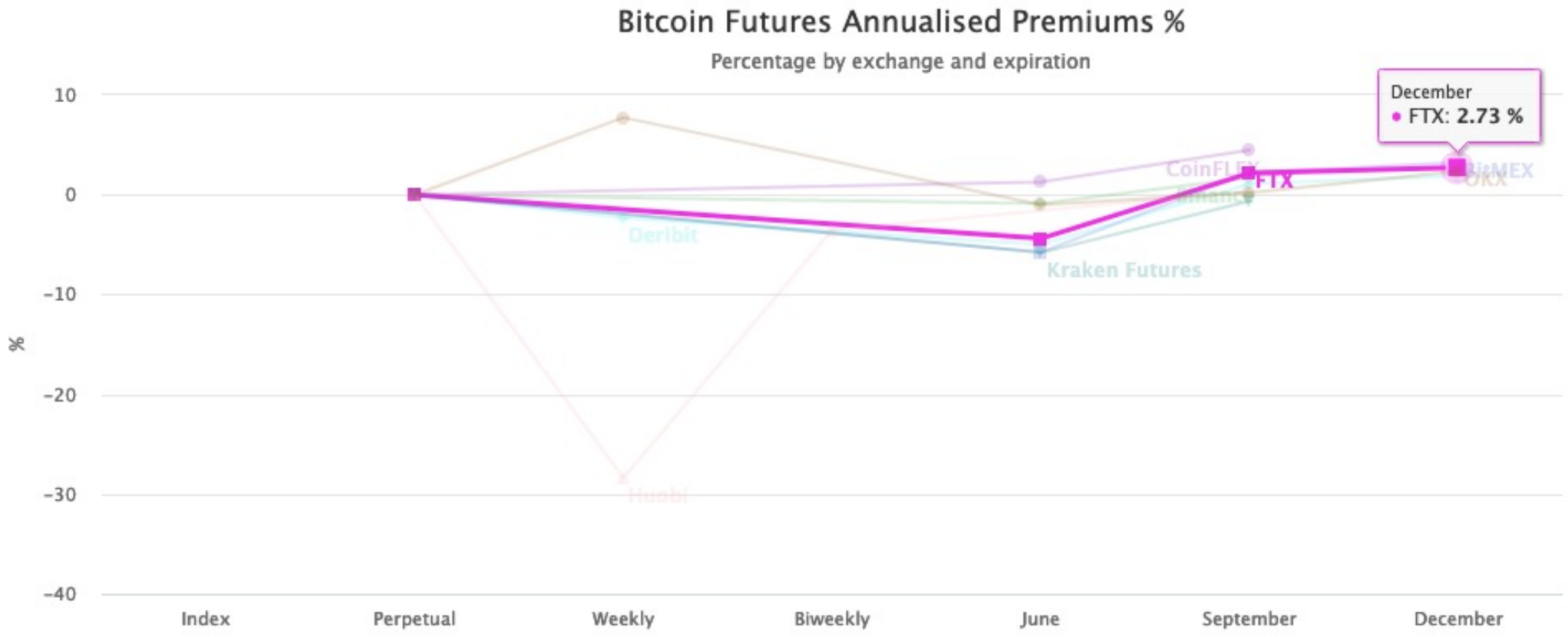
Hedging methods

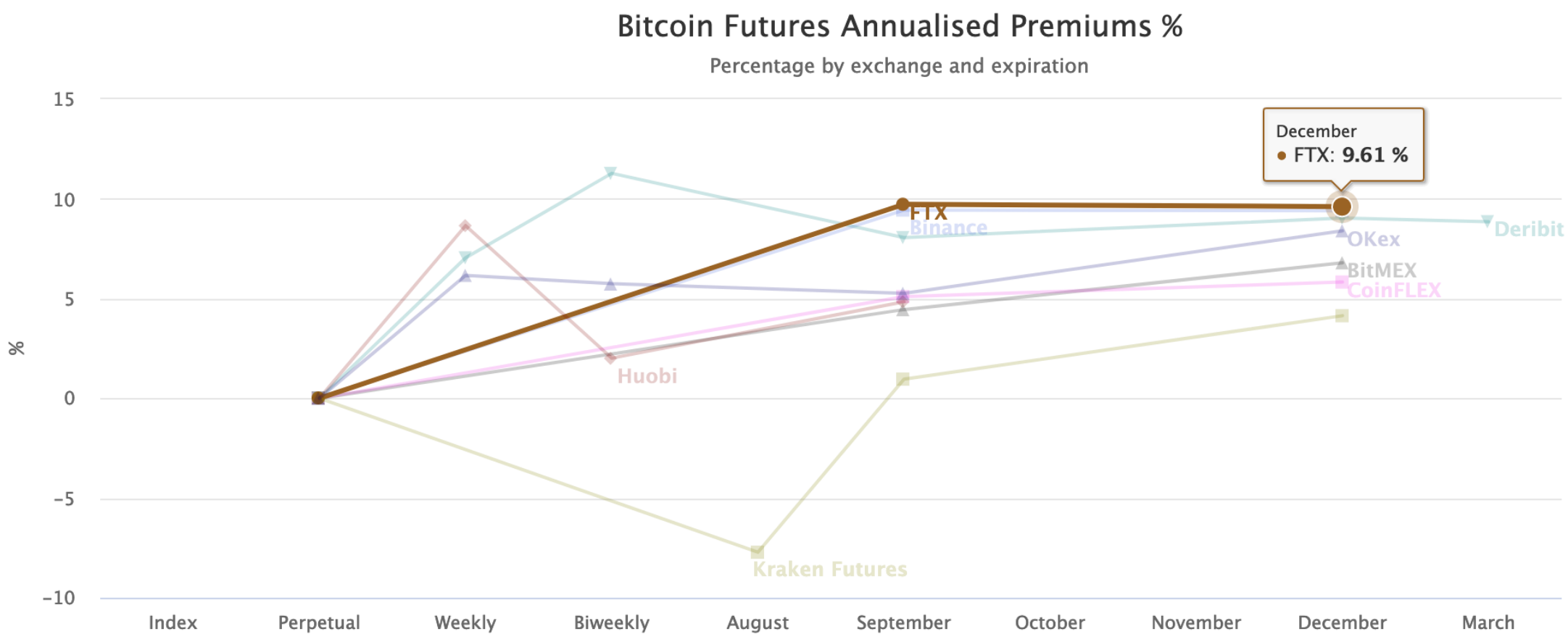
Futures

- The risk of an exchange hack/crash/rugpull
  - ...but on the exchange you just need to have collateral (~20%-30% if you don't want to deal, < ~15% if you automate)
  - Not just a security risk, but also a KYC risk
- Earns direct funding rate/contango
- FTX and Coinex have XMR perpetual swaps
- You can hold most your assets in XMR or BTC, which you can directly sell. No need to do an exchange with every trade

Stablecoin

- Stablecoin risk
  - Smart contract / Tether / regulatory risk
  - Will it hold the peg?
- It can be completely on a hardware wallet
- If you want to earn interest, another risk of some defi project (aave, ...)
  - Not just a security risk, but also a fee risk, interest rate risk
  - All the money that earns interest rates is in the DeFI smart contract
- Nice project that has stablecoins, some privacy, integrated DEX with direct XMR off-ramp is Incognito


Bitcoin Futures Annualised Premiums %
Percentage by exchange and expiration
December
FTX: 2.73 %
10
0
-10
-20
-30
-40
%
CoinFLEX
FTX
BitMEX
OKX
Binance
Deribit
Kraken Futures
Huobi
Index
Perpetual
Weekly
Biweekly
June
September
December


Bitcoin Futures Annualised Premiums %
Percentage by exchange and expiration
15
10
5
0
-5
-10
%
December
FTX: 9.61 %
FTX
Binance
Deribit
OKex
BitMEX
CoinFLEX
Huobi
Kraken Futures
Index
Perpetual
Weekly
Biweekly
August
September
October
November
December
March

Asset	Total supplied	Supply APY	Total borrowed	Borrow APY, variable
DAI DAI.e	420.40M $ 420.93M	2.92 % 1.50 %	336.12M $ 336.55M	4.08 % 0.47 %
USD Coin USDC	1.84B $ 1.84B	2.41 % 1.18 %	1.42B $ 1.42B	3.49 % 0.38 %
Tether USDt	183.55M $ 183.37M	9.26 % 1.46 %	168.96M $ 168.80M	17.72 % 10.23 %

Why Monero?

- Vekslák does not want to deal with tainted coins
    - Lightning network could solve this problem, but then there‘s problem of liquidity and channel opening fees
- Vekslák does not want to expose their transactions on-chain
    - I have bought fiat from a Vekslák and with one click I have seen all his trades – he has been reusing the address (of a centralized exchange)
    - Also connecting transactions is a problem
- Waiting for confirmation for 5-30 minutes is not fun, especially in cold or rain. Monero‘s first block confirmation is fast
- You get Lightning privacy with hardware wallet security
- Whatever anyone does with the coins is their business and you cannot be blamed for an exchange refusing the coins – Monero is fungible, so if it confirms, it‘s good, all transactions are final

Privacy preserving dollar-cost-averaging (DCA)

- Buy crypto for higher amount (ATM, vekslák)
    - You can buy when exchange rate is high and people want to cash out, earning a premium for yourself
- Hedge crypto to USD, ideally earning interest rate
    - Option 1: convert to stablecoin
    - Option 2: open a short on BTCUSD, XMRUSD futures – you can combine timed and perpetual swap for optimal interest rate
- Every month (week) unhedge the same dollar amount
    - No bank transfers involved, privacy preserved
    - Your ass sits comfortably on your chair most of the time
    - First step earns you premium, second step earns you interest rate

Balancing the sides

If crypto prevails...

- A vekslák can become a proxy merchant
  - Discounted gift cards for crypto - who wouldn't want 10%-30% off anything from Amazon?
- Provide a dollar interest-bearing account for the family

If fiat prevails

- Crypto-secured interest-bearing loans
- Sell your services, teach people crypto

Conclusion

01

Money is the memory of the good deeds of society

02

The main memory can go bad (countries and their central banks are working hard to make it unusable)

03

It's good to have a record of good deeds in a backup memory

- Vekslák makes these records available
- Vekslák is a protection against bad regulation
- Vekslák provides privacy and education
- Any crypto enthusiast who has a bit of spare cash can provide this service alongside other activities
- Veksláks are returning the peer to peer nature to crypto

Lectures and resources

Volatility, strategies: https://bit.ly/volatilitybitcoin

Financial surveillance and crypto utopias:
https://bit.ly/financialsurv

Crypto trading groups

https://juraj.bednar.io/cryptotradinggroup

Vekslák course (currently Slovak, will be in English, write me if you are interested):

https://juraj.bednar.io/eticky-vekslak

Futures (derivatives)

- Coin-margined inverse perpetual swap
- Coin-margined inverse future with expiry
- Contract to buy/sell the crypto in the future
  - With the settlement of the purchase price in crypto
- The most common hack:
  - Buy Bitcoin (long)
  - Buy future Bitcoin (short)
  - I have Bitcoins in stable dollar value (something like a stablecoin)
  - Most of the time I get paid to hedge

I want to hold fixed $1000 in BTC (crypto-fiat)

Now the exchange rate on the future is 50000$ for 1 BTC, expiration in December.

With 1000$ I buy 1000/50000 = 0.02 BTC

I open short for $1000 on BTCUSD coin-margined future (perpetual swap)

December: BTC rose to $60000

The contract on the derivatives exchange closes with a minus of 0.003333 BTC

So I have .01666 BTC, which is 0.01666*60000=1000$

(0.02 from spot trade minus 0.003333 from the future)

December: BTC dropped to $30000

The contract on the exchange closes with a plus of 0.01333 BTC

0.02 from spot + 0.01333 from future = 0.03333 BTC

0.03333 * 30000 = 1000$

How to use the future contracts?

To be able to do "counter-trade" without having to send dollars/euros somewhere - and remain price-neutral

To earn the funding rate

To be able to provide a counterparty even in a very extreme situation (buying bitcoin when everyone wants to sell and vice versa)

To be able to trade BTC for fiat without a bank transfer

Funding rate / contango

- Interest for holding a short position
- The vekslák is waiting for a trade, he should be compensated for holding fiat
    - Inflation is a (insert your favorite dirty word here)
    - When a vekslák is waiting for a trade, he is still providing a service, holding crypto/fiat that he is ready to sell/buy at a worse rate for him
    - Funding rate/contango is the interest dependent on the time he is holding fiat-hedged crypto