Cover Slide:

Hello everybody, I am Timothy McWilliams, I am Dan Freeman, I am Sudip Bhattacharyya. Here is our topic for today’s presentation - “Enhancing Trust in the Cryptocurrency Marketplace: A Risk Scoring Approach”.

Slide 2:

What is cryptocurrency? Cryptocurrency is a digital asset used as a medium of exchange and enabled by cryptography to secure transactions and verify transfer of assets.

Slide 3:

Unlike conventional currencies, cryptocurrency has no physical currency, no centralized control, no intermediary. It offers complete anonymity of users and transactions are immutable or irreversible.

Slide 4:

We see more than 1500 cryptocurrencies in today’s market. Few popular ones are – Bitcoin, Litecoin, Ethereum, Monero, Dash, Ripple etc.

Slide 5:

As of Q1, this year, crypto market was valued at more than $400 billion. It reached record high at $600 billion by end of 2017.

Slide 6:

Bitcoin is the highest share holder in cryptocurrency market. Until 2016 their share was more than 80% which came down to 40% in recent times because of emergence of other currencies.

Slide 7:

Blockchain was first introduced by Satoshi Nakamoto in 2009. It is a platform that runs Bitcoin and other cryptocurrencies marketplace. It is a peer-to-peer network with no centralized control and trust is built based on cryptography.

Slide 8:

This slide shows a comparison between centralized, decentralized and distributed ledger architecture. The right most one is distributed where all transactions are visible by all the parties in the network.

Slide 9:

This shows a typical transaction cycle in blockchain network, how a public-private key infrastructure ensures trust and security for blockchain.

Slide 10:

In blockchain identities are masked by hash values. Transactions are immutable, cannot be reversed once added. Distributed architecture significantly reduces chances of attacks.

Slide 11:

No system is fully secured. In spite of being trustworthy we have seen multiple hacks and scams in crypto market and few are displayed here.

Slide 12:

Why hack happens? Firstly because of lack of regulations – no KYC process in place and no mandatory AML report. Also offenders take advantage the anonymous nature of blockchain.

Slide 13:

And that’s our objective to make it more secure. Build a trust mechanism in terms of risk score which enables users to avoid risky parties while making transactions.

Slide 14:

The risk score will empower users with a self-guided trust. No dependence on any third parties.

Slide 15:

The process starts with creating a blacklist, sample transactions, assign risk factors, profile transactions with machine learning, validate models, build risk scores.

Slide 16:

Our blacklist contains the hashes from historical hacks and thefts. Profile them will allow us to identify such transactions in future.

Slide 17:

Our raw database has all bitcoin transaction until February 9, 2018. It has block level and transaction level details. Over 300 million transactions.

Slide 18:

Our database has 9 tables and this slide shows the schema – the structures of the tables and relations and mapping between them.

Slide 19:

We have taken a sample from our raw data. Assign a risk factor of 1 for all historical hacks and 0 for the rest. Sample data has 8,109 records – 2,172 hacks and 5,937 non-hacks.

Slide 20:

Here are the modeling approaches. We have done Random Forest, K-Nearest Neighbors and Support-Vector Machine. Ran baseline models with 80/20 splits and did feature engineering.

Slide 21:

Random Forest is an ensemble method creating multiple trees. Here in picture Tree1 classifies as win, Tree 2 as win and Tree 3 as loss. So, the final result is win for being the model value in the individual tree result.

Slide 22:

These are random forest results. 7 features. 99.81% accuracy. Misclassified only 3 out of 1,193 non-hacks. All hacks are classified rightly.

Slide 23:

These are the key features. Number of transactions in a block is the most important followed by number of inputs and the input amount.

Slide 24:

In KNN, unknown is classified as majority of neighbors. In the picture if K=5, then unknown is classified as blue triangle, otherwise as red star.

Slide 25:

KNN produced results with 99.88% accuracy, misclassified only 2 non-hacks. Line graph shows mean-square error increase with K which implies that low values of K are better.

Slide 26:

This is the visualization of result from KNN. Blue is the hack area and Orange is the non-hacks area.

Slide 27:

This slide talks about SVM. SVM creates a hyperplane which becomes a straight line or curve for 2-dimensional. Support vector is calculated based on maximum margin.

Slide 28:

SVM model built with top 2 features – Number of transaction in block and number of inputs. It gives 86% accuracy. More realistic.

Slide 29:

Here is the visualization of SVM results. Blue indicates hack area and orange shows non-hacks.

Slide 30:

Risk score indicates trustworthiness of a user. Scores assigned against each address ID. It is defined as

Total number of high risk transactions by Total number of transactions.

Slide 31:

Here we have explained how risk score is calculated. It all depends on transactions profiled based on ML algorithms.

Slide 32:

Our random forest and KNN models are overfitted. It happened because of very low number of hacking incidents which lacks diversity. SVM is more realistic and it classifies all hacks correctly which more important.

Slide 33:

With more time and a better infrastructure, we expect to scale up our work which could be extended to all 300+ millions of transactions. Also, we would like to add more features like type of exchange and mining characteristics for transactions.