# Introduction to Bitcoins: A pseudo-anonymous electronic currency system

**Co-Chairs:** Sergio Martins, IBM Canada Ltd.; Yang Yang, IBM Canada Ltd.

**Theme:** Next Generation Systems

**Integrated Solution:** Smarter Commerce

**Abstract:**

- Electronic financial transactions and payment systems have traditionally relied on third party institutions, such as banks or credit card companies, to ensure secure transfers between parties. Users of such systems must trust that third party institutions will be honest and follow through with their claims. Trust-based systems are difficult to establish in the digital realm without a governing body regulating and securing transfers. Systems using this model have many downfalls that make them risky and undesirable for Internet use. With the requirement of all transactions being completely digital, how can we transfer funds securely without a trusted third party?
- All types of currencies share many common problems such as stability, control, and inflation. As time passes, the relative value of a currency usually decreases (meaning that prices increase). If this happens too quickly, it can cause major problems if prices increase beyond the means of the populace who uses the currency. Another problem is stability because the currency should not be subject to dramatic exchange rate fluctuations under the influence of a single individual or party. Control over a currency, or lack thereof, is also important. Typical fiat currencies depend on a mint and the promise that the mint will continue its operations. If the mint were to close indefinitely, the currency would likely die out in a relatively short period of time. Therefore, the mint has some level of control over the currency.
- Bitcoin is a digital currency introduced in 2009, based on a self-published paper by Satoshi Nakamoto[1]. Bitcoin enables payments that are based on proof, rather than trust, in a manner that is similar to cash. A seller given a cash payment can inspect the currency and, with a good degree of confidence, assert whether the payment is valid or invalid. Bitcoins works using a similar concept that make coins and coin ownership easy to verify. An important difference between this virtual currency and typical fiat currency is that Bitcoin's validity can be verified.
- During this workshop we showed attendees the verification process as well as the algorithms and technologies that make verification possible. The audience learned about online money transaction, then analyzed standard techniques and form comparisons between them. The workshop then proceeded to discuss the history and purpose of Bitcoins along with an overview of its concepts and terminologies.
- The workshop continues to compare Bitcoins with other transaction techniques discussed and talk about the pros and the cons. We also go though the problems that Bitcoin will be able to solve and what new problems it will introduce.
- Attendees will learn the details of Bitcoins and its implementations. From Asymmetric cryptography algorithms to hashing and digital signatures to proof of work, the audience will be walked though all the technologies that make Bitcoin possible.
- The workshop will take attendees through actual Bitcoin transactions and the details of the transaction process as it will allow them to see how the Bitcoin system overcome problems such as double spending. The audience was also taught about Bitcoin generation and how Bitcoins are generated out of thin air. For context, we covered how much coins are worth and how people are already profiting from services other than mining. The details of Bitcoin "blocks" and "chains" were demystified in a manner that was detailed but simple to understand.

- The Bitcoin network was one of the main focuses - how a distributed and completely public network can maintain the anonymity of its users. It was discussed in detail about how transactions are validated through the network and about the transaction databases that is on the distributed network. The audience learned how the distributed database handles failures, delay, and is able to work effectively with only a subset of the entire database. The audience learned concepts such as merkle trees and how they help the Bitcoin network to maintain the database. We answer questions such as how Bitcoins control the expansion of its own currency when the Bitcoin network may double in size in a short period of time. The many interesting characteristics of the network were unveiled during this engaging demonstration.
- Attacks and malicious hosts are constantly a threat to modern day electronic transactional systems and this also applies to Bitcoin. We mapped out the architectural features that make Bitcoin naturally resilient to many common attacks, as well as the features that make it vulnerable. We discussed possible attacks on the Bitcoin network as well as attack mitigation and ways in which end users can protect themselves.
- Another interesting issue is anonymity. Bitcoin is regarded as being anonymous by many people, yet Bitcoins can be traced from the original miner all the way to the current owner. A Bitcoin address itself is just a number and cannot identify anyone. However if a person manages to collect enough information about the owner of that address (perhaps through forums) then the owner can be exposed.
- To conclude, in this workshop we explored everything from cryptographic algorithms to the massive peer-to-peer network. We took a security perspective for an in-depth exploration of Bitcoin attacks and attack mitigation. We ended our workshop with a look at how Bitcoin might change the e-commerce landscape, followed by an open discussion.