Privacy and Security Concerns for Online Share Trading

J. Trevathan and W. Read

Abstract — Online share trading has made investing in share markets more accessible to novice traders. Investors can trade from the comfort and privacy of their own homes. However, there are many inherent risks in online share trading. Share markets are becoming the target of new elaborate scams, terrorist attacks and corporate crimes. This paper provides an overview of privacy and security for online share trading in the context of auctions. We discuss the additional parties involved, and how their individual requirements affect auction security and privacy. We give a description of share market related crimes and their implications for online trading. We investigate existing security mechanisms and cryptographic solutions to these problems. This paper presents an auction scheme for anonymous and secure share transactions.

Index Terms — Continuous Double Auction, Cryptography, Insider Trading, Online Broker, Share Market

1 Introduction

Brokers (such as Commsec[1]) now offer a multitude of online services to small traders for accessing the world's financial markets. Online traders perform an ever-increasing number of share market transactions. Share markets such as the New York Stock Exchange[2] and the Australian Stock Exchange[3] use an auctioning mechanism referred to as a Continuous Double Auction (CDA). This is an auction that has many buyers and sellers continuously trading a commodity. In an online share trading system, traders are the bidders and the Share Market is the Auctioneer. However, unlike a regular auction, bidders must submit their bids to the Auctioneer via a Broker. The Broker earns a commission for its services.

Despite online share trading's popularity, there are security and anonymity concerns regarding the integrity of the participants, and the auctioning process. Share markets are tightly regulated. However, many of the problems inherent in online share trading, are similar to the problems encountered by more conventional online auctions such as eBay[4]. For example, a trader might repudiate having made a bid, or refuse to pay for, or deliver shares. Furthermore, the Broker/Auctioneer could be corrupt and initiate unauthorised trades. In addition, much information is revealed about an individual, including his/her personal information (identity, address, etc.), and trading history. Such information could potentially be used against him/her, or for marketing purposes.

This paper provides an overview of online share trading in the context of auctions. We discuss the additional parties involved, and how their individual requirements affect auction privacy and security. We provide a description of share market related crimes and their implications for online trading. We also investigate existing security mechanisms and cryptographic solutions to these problems. Finally, we present a scheme for anonymous and secure share transactions.

2 Online Share Trading

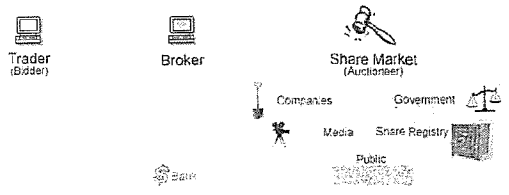

Fig. 1. The Online Share Trading Process

Figure 1 illustrates the major parties involved in the share trading process. In order to trade shares, a Client must first obtain an account with a Broker. This is usually done offline via a form. Once registered, the Broker issues the Client with a Client Number. This number

- *J. Trevathan is with the School of Mathematics, Physics and Information Technology, James Cook University, Australia. E-mail: jarrod.trevathan@jcu.edu.au.*
- *W. Read is with the School of Mathematics, Physics and Information Technology, James Cook University, Australia. E-mail: wayne.read@jcu.edu.au.*

[1] http://www.comsec.com.au
[2] http://www.nyse.au
[3] http://www.asx.com.au
[4] http://www.ebay.com

is unique to the Client (i.e., no two clients have the same number). The Client enters his/her bid via computer. This is communicated to the Broker's computer and is then entered into the Share Market.

This is analogous to online auctions where the Trader is a bidder, and the Share Market is the Auctioneer. However, unlike a regular auction, a bidder submits a bid to the Auctioneer via an intermediary (i.e., the Broker). Furthermore, the Share Market is a more complicated entity than a regular Auctioneer. The Share Market consists of numerous parties with differing interests in the auction proceedings.

Figure 1 also shows the additional parties involved in trading shares. A Company issues shares to the Share Market in order to raise capital. The Company releases statements to the Media, such as profit reports or market sensitive announcements. The Public observes the Share Market for potential investment opportunities, or for entertainment. It is also the Broker's role to provide clients with information regarding the market, and/or advice concerning when to buy or sell.

At the end of a completed transaction, the Broker debits or credits a Client's bank account. The Share Registry is a trusted authority tasked with keeping records on share transactions and ownership. The Government is able to use the Share Registry to ensure that bidders have paid taxes on their transactions, and to check compliance with disclosure and ownership laws. Furthermore, companies require some record of who their shareholders are. This is to facilitate dividend payment, allow voting at shareholder meetings, and dissemination of market information.

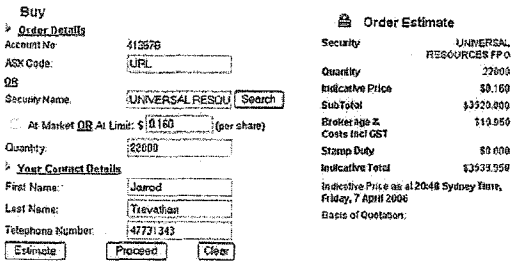

Fig. 2. An Example Buy Bid Used in Online Share Trading

Brokers allow clients to enter new bids and to modify/cancel existing bids. Figure 2 shows a typical web form a Client would use to submit a buy bid. (Note that a sell bid is just the opposite.) First a Client provides his/her Client Number, so that the Broker can link the order they submit to them. Next, the Client enters either the company code, or the full name of the company they want to purchase shares in. The company code is unique to a company, and is used for identification purposes.

There are two options for entering the price at which the Client wishes to purchase shares. With an "at limit" order, the Client enters the exact price they are willing to buy the shares at. When the Broker acts on the order, they will purchase the shares at a price no higher than the limit the Client has specified. Alternately, an "at market" order instructs the Broker to purchase the shares from the next available seller, regardless of the price. Next, the Client enters the quantity of shares they want to buy. The Client is also required to enter some personal information about themself including first name, last name and phone number.

The right side of Figure 2 gives an estimation of the Client's buy order. For this example, the Client has specified that they want to buy shares in Universal Resources (URL). The Client desires 22,000 units at a limit of $0.16, thus the basic trade's total value is 22,000 X $0.16 = $3,520.00. The Broker also adds commission of $19.95. This brings the total price that the Client must pay to $3,539.95.

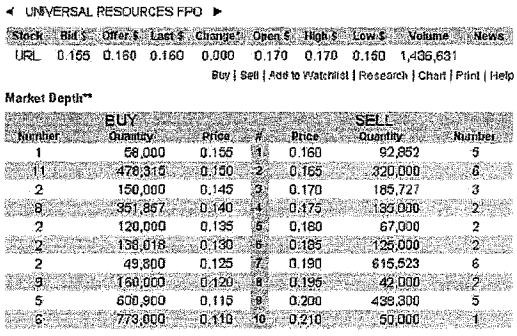

Fig. 3. A Example Market Depth Indicator which Lists all the Buy and Sell Bids for a CDA

Figure 3 shows a market depth indicator, which lists all the buy and sell bids grouped according to price. The quantity is the aggregate of all bids at the particular price level. Every time a Client submits a new order, this information is immediately reflected via the market depth. Market depth information is available to all traders. When a trade is executed, the Broker notifies the Client via e-mail.

5 Privacy and Security Issues Inherent in Trading Shares Online

Auction security issues have been fully discussed in [2], [3], [4], [5] and [7]. Shares are traded in an auction type referred to as a Continuous Double Auction (CDA). Therefore, online share trading exhibits similar problems to conventional online auctions. However, a CDA is much more complicated, as there are many buyers and sellers continuously trading a commodity. This requires a more sophisticated clearing process (i.e., the manner which buy and sell bids are matched). Furthermore, the additional parties involved in the share trading process make it difficult to clearly define privacy and security requirements.

6.1 Privacy Concerns

In existing 'secure' auction schemes, privacy is regarded as a fundamental design goal. This is due to profiling, where the Auctioneer or seller uses a Client's information to force them into paying a higher price. For example, if a bidder's true valuation is discovered, then the seller may set the auction's reserve price at this amount. Alternately the seller may engage in shill bidding to artificially inflate the auction's price to the bidder's valuation thus ensuring maximum profit. Online Brokers have largely neglected anonymity issues. The current approach lets the Broker and share market learn all information regarding the Client and his/her order. This is undesirable as personal information can be abused, or used against an individual.

If a Client has a high profile, they might want to conceal the fact that they are bidding. This might occur in the case where the Client feels that their privacy would be compromised in some manner (e.g., reveal that they have a fetish for an item), change other bidders' perceptions of the item (e.g., stimulate unwanted bidding), or influence the seller to raise the commodity's price.

It is common for companies to sell client information to marketing agencies. Such information can include names, addresses, account and portfolio balances, and historical trading data. This often results in an individual being profiled and targeted with junk mail. For example, a Client may continually be solicited by offers for credit cards, investment trusts, or share market tip-sheets.

Furthermore, shareholders could be harassed during disputes involving the company. For example, during strikes, or if the company is engaging in unethical behaviour. Unethical behaviour may include pollution or selling products that cause harm (e.g., cigarettes, weapons, products containing asbestos, etc.). Furthermore, in the event of a hostile takeover, shareholders of the company being taken over may be harassed by the takeover advocates. It should be up to an individual whether or not they want to be associated with his/her share holdings in these situations.

However, the need for privacy must be balanced against the propensity for clients to cheat. Identity escrow (or recovery) is required in the situation where the Client has acted illegally. In this situation, it is often necessary for regulatory authorities to trace past transactions. Furthermore, there are purposes related to Government and auditing procedures that may require an individual's identity to be recovered.

6.1 Security Concerns

The most pressing security problem in online share trading is that there is no means for a Client to verify whether his/her order has been submitted to the Share Market. A dubious Broker might alter a Client's order (thereby defrauding the Client), or block it in the case where s/he disagrees with the Client's judgement, or has a vested interest in some aspect of the trade. As the Broker gains a commission proportional to the quantity traded, they might buy or sell a larger portion than warranted.

A further concern is that there is no evidence that the Share Market has included the order in the auction. Nor is there any verification of how the orders are being matched. Bidders must rely on market depth indicators. However, there is presently no means of recourse if the bid does not appear, nor if it was matched in a manner inconsistent with the clearing rules.

The Broker and Share Market must also be able to verify that the Client submitted the order. Otherwise, the Client may repudiate having made the bid. Furthermore, lack of authentication makes it possible to forge an order and hence frame innocent clients. For example, the Broker or Auctioneer may forge an order on a Client's behalf, or an outsider that wants to cause financial hardship to a Client.

Online share broking schemes use various solutions to enforce payment including credit, client accounts and fines. Credit allows clients to submit buy bids up to a set credit limit. If the bid is cleared, the Broker requests payment from the Client's Bank. Another solution requires clients to hold accounts with the Broker, and only allow bids up to the value of the account balance. When a Client submits a buy bid and this bid is cleared by the auction, the bid value is withdrawn from the Client's account. Alternately, if a sell bid is cleared, the value of the bid is deposited in the Client's account. Finally, Brokers can impose fines for defaulting on payment, and can sell winnings in an attempt to recuperate unpaid money.

However, none of these solutions are perfect. Credit limits provide the Client with less restrictions, but requires the Broker to place some confidence in the Client's ability to pay. A Broker held account prevents risk on the Broker's behalf, but can be restrictive to the Client who might want to hold the account funds elsewhere while not in use. For example, if a Broker offers a lower rate of interest compared to another financial institution, the Client might want to move the funds to the better paying account when the funds are not being used. Fines and selling off goods won is a last ditch effort only taken to either deter or recover lost money after a Client has defaulted on payment.

An additional concern is that a Broker might not debit/credit the Client's bank for the correct amount. While this may appear to be extreme, and the reader may be thinking, "this wouldn't happen in real life", consider what would happen if it did. What means of recourse does a Client have? Essentially it would be the Client's word against the Broker's word, and it would require auditing the trade history and litigation to resolve. Once again, this comes down to a Client's ability to authenticate his/her bids and verification of the auction proceedings.

6.1 Share Market Crimes

The share trading process has many unique crimes compared to conventional online auctions. *Insider trading* generally refers to buying or selling a security (shares), based on the knowledge of non-public information. The insider has a fiduciary duty or relationship of trust and confidence regarding the security. For example, a company CEO sells all his/her shares prior to, and with knowledge that the company is about to go bankrupt. In this situation the CEO has acted illegally, as the Share Market does not yet know such information. A recent high profile individual to be convicted in the U.S. of insider trading is Martha Stewart[5].

Insider trading violations may also include *"tipping"* such information, securities trading by the person *"tipped"*, and securities trading by those who misappropriate such information. Rene Rivkin[6] (in Australia) was convicted of insider trading when he acted on a tip provided by a QANTAS executive. Rivkin allegedly sold his QANTAS share holdings in anticipation of bad market related news, thus avoiding any loss when the news later became public.

Other share market crimes involve *misinformation*, where a company influences its share price by announcing incorrect statements regarding its financial standing. Furthermore, Brokers or financial advisers might be in possession of shares, which they sell to their clients for a profit using misinformation. *"Ramping the market"* refers to actions designed to artificially raise the market price of listed securities and to give the impression of voluminous trading, in order to make a quick profit. Once the bidding slows, the price falls back to its original, thus depriving those who purchased shares during the hype.

6.2 Existing Mechanisms for Ensuring Privacy and Security

Existing online trading sites only require clients to log-in using a Client Number and password. Once logged in, application level encryption is used to secure the session. The log-in usually times out after a period of inactivity, which is useful in the case where a Client leaves his/her computer for a long time, or forgets to log-off. Privacy is enforced by a privacy agreement among the Broker and Client. The Government provides policing in the form of regulation.

A Regulatory Authority is a law-enforcement entity that governs share market behaviour. Table 1 lists some of the World's major

[5] http://www.sec.gov/news/press/2003-69.htm

[6] http://www.wsws.org/articles/2003/jun2003/rivk-j07.shtml

authorities. These authorities have the power to prosecute, incarcerate, fine or ban individuals guilty of share market crime. Such authorities were originally created to regulate conventional offline trading. Online share trading's similarity to online auctions means that authorities must be capable of preventing auction-related fraud. However, this seems doubtful if commercial online auctioneers are unable to solve the problem.

Table 1 Regulatory Authorities around the World

Country	Authority Name
Australia	Australian Securities and Investments Commission
Canada	Ontario Securities Commission
China	China Securities Regulatory Commission
France	Commission Des Operations De Bourse
Germany	Bundesaufsichtsamt Fur Den Wertpapierhandel
Israel	Israel Securities Authority
Japan	Securities Bureau of the Ministry of Finance
Russia	Federal Commission for the Securities Market of the Russian Federation
United Kingdom	Financial Services Authorities
USA	U.S. Securities and Exchange Commission

Further concerns regarding trust also cast doubt over a Regulatory Authority's effectiveness. In reality, a Regulatory Authority is just another individual that is involved in the auction process. It is no more trustworthy than anyone else. Some individuals have even felt that authorities have had unfair bias or vendettas against them. Furthermore, such authorities are too expensive to maintain and to seek recourse through. The authority must be funded or raise money to continue running. This ultimately makes the authority biased towards the funding source. Additionally, an authority is only effective to police large-scale fraud, whereas, the process is too complicated and expensive for small fraud instances. The question could be asked, "Are regulatory authorities doing enough to protect the privacy and rights of individuals"?

7 Cryptographic Mechanisms for Conducting Anonymous and Secure CDAs

Cryptography can be used to provide bid authentication and privacy in auctions. Most existing auction security proposals have focused on sealed bid auctions (e.g., see [2], [7]). Wang and Leung [8] proposed a scheme for private and secure CDAs. However, this scheme has several security concerns and is not specific to share markets. Trevathan *et al* [5] propose a CDA scheme, which uses a cryptographic mechanism referred to as a *group signature*. A group signature alleviates many of the security and anonymity problems described in the previous section. To understand how a group signature works, we first provide some background on more general cryptography.

Cryptography allows two parties to communicate over an insecure medium (such as a network). This is achieved by encrypting a message using an encryption algorithm and a key. The message is decrypted at the receiving end using a decryption algorithm and the key. As long as an eavesdropper doesn't know the key, he/she can't read the message. There are two main types of cryptography: private and public. *Private key* cryptography uses a single key to encrypt and decrypt a message. When encrypting/decrypting a message, both sender and receiver must possess the secret key. This process is shown in Figure 4 A.

Alternately, *public key* cryptography uses two keys, one for encryption and the other for decryption. The public key is made available to everyone and is used to encrypt messages. The private key is only known by the receiver and is used to decrypt messages. In general, it is hard to learn any information about the private key using the public key. This process is shown in Figure 4 B.

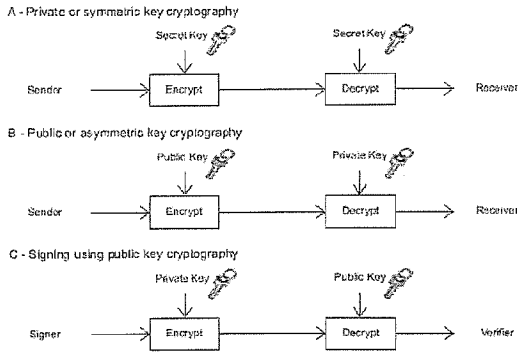

Fig. 4. Public/Private Key Encryption and Digital Signatures

A digital signature allows the sender to sign a message such that the receiver can authenticate that it originated from the sender. This provides proof of the signer's identity and prevents repudiation of the

signed message. Public key cryptography can be used to sign messages (Figure 4 C). The sender signs the message using his/her private key. The receiver can then verify the signature using the sender's public key. As only the sender knows his/her private key, the message could have only originated from him/her.

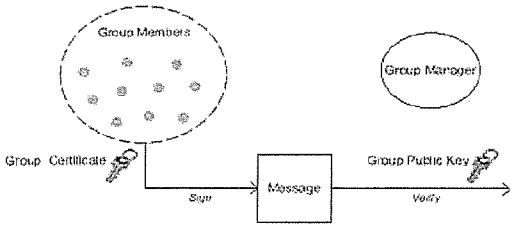

Fig. 5. Group Signature Scheme

A group signature scheme allows group members to sign messages on the group's behalf. Anyone can verify that the signature is authentic using the group's public key. However, it is not possible to determine which group member signed the message. To join the group, a user must register with a Group Manager (GM) (see Figure 5). The GM is responsible for issuing group members with a private key and maintaining the public key. In the case of a dispute (e.g., a member denies having signed a message) the GM can trace the signer's identity.

Group signature schemes naturally lend themselves to auctions. In this case a bidder belongs to a group of bidders. A bidder can sign bids on the group's behalf in such a manner that s/he remain anonymous. The Auctioneer can verify the signature on a bid using the group's public key. The group signature prevents bids from being forged, and allows the bidder's identity to be

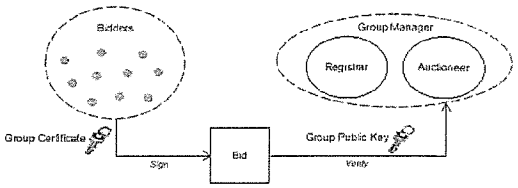

Fig. 5. An Auction Scheme Based on a Group Signature Scheme

revealed if a bid is repudiated. However, in terms of an auction, the Auctioneer is not the appropriate choice for the GM. The GM is generally trusted and therefore the Auctioneer cannot perform this role, as they could cheat by revealing a bidder's identity without due cause.

The Trevathan *et al* [5] CDA employs a group signature scheme to allow for anonymous bid submission. The scheme introduces a Registrar that is responsible for registering bidders. Figure 6 shows the modified group signature scheme. A bidder registers with both the Auctioneer and Registrar in a manner such that his/her identity is split between the two parties. Neither the Auctioneer nor Registrar individually knows the bidder's identity. A bidder remains anonymous as long as both parties don't collude.

The CDA protocol is presented in Figure 7. The arrows represent the messages sent between parties. Dashed circles surrounding messages indicate that the enclosed messages are sent during a particular stage of the auction protocol. The basic protocol for the CDA scheme is as follows:

- ***Registration:*** A bidder first registers with the Auctioneer supplying his/her ID. The Auctioneer issues the bidder with a

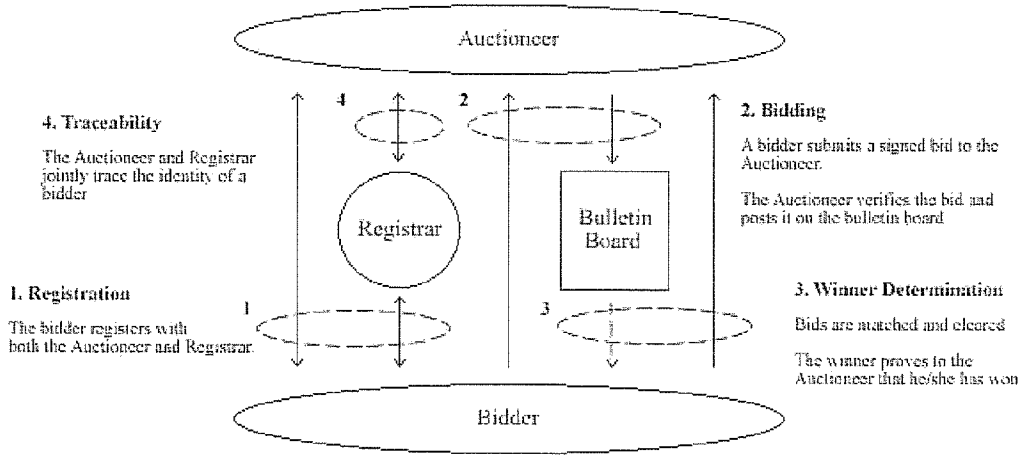

Fig.7. The Basic CDA Protocol

signed token. The bidder presents this to the Registrar. The Registrar verifies the signed token and issues the bidder with a group certificate.

- ***Bidding:*** A registered bidder signs a bid using his group certificate. The bid is then submitted to the Auctioneer. The Auctioneer checks the bid to ensure that it is correctly submitted by a legitimate bidder. Signed bids are posted on a public bulletin board. This can be considered as a web page that every one has read permission, but only the Auctioneer can write to. This allows participants to observe and verify the auction proceedings.
- ***Winner Determination:*** The Auctioneer determines the outcome of the auction according to the auction's rules. A bidder can verify they have won by reproducing the signature on the winning bid.
- ***Tracing and Revocation:*** The Auctioneer and the Registrar combine their information to determine a bidder's identity, and if required, to revoke them from the auction indefinitely.

7 Secure and Anonymous Online Share Trading

The Trevathan *et al* [5] scheme is specific to CDAs and does not address concerns involving the Broker. In this section we define the Broker's role in relation to a Client's privacy and security. We propose an extension to [5] that takes account of the Broker's requirements and responsibilities.

The relationship between a Client and the Broker presents new security problems that have not been previously discussed in auction security literature. One such concern is that a Client needs to know that his/her bid has been passed on to the Auctioneer. For example, a corrupt Broker might deliberately block a Client's bid if they don't want them to initiate a trade. This might happen if the Broker thinks that the Client's judgement is unsound and is acting in a manner inconsistent with the Broker's advice. Alternately, the Broker might have malicious plans for the Client's holdings for a share market related crime such as ramping the market. A further security concern is regarding the Broker's ability to initiate unauthorised trades on a client's behalf. As a Broker knows a Client's personal information, there is nothing preventing them from forging a bid. The bid still appears to be genuine to the Auctioneer.

The Broker and Client share a unique relationship, which differs from the Auctioneer/Client relationship. Although the Broker and Client mutually distrust each other, there is some requirement for trust as the parties benefit from cooperation. (I.e., the Client makes a trade and the Broker collects a commission.) These requirements make it difficult to define a clear privacy policy between the Broker and a Client.

As a Broker is providing a service to the Client, operational requirements dictate that a Broker knows certain facts regarding the bids submitted. For example, to determine the Broker's commission and which Client to collect payment from. In addition, the Broker must manage a Client's portfolio and therefore knows everything about the Client's trading behaviour. Therefore, the privacy requirement must be relaxed between a Client and the Broker. Instead, privacy between the Broker and a Client can be enforced with a non-disclosure agreement. Although this is not ideal from an anonymity perspective, it is still an improvement on allowing the Auctioneer and market observers full access to private information.

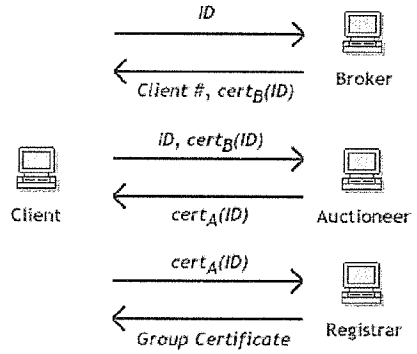

Fig. 8. CDA Registration Protocol Incorporating a Broker

Figure 8 shows an extension to the registration procedure of [5]. This modification incorporates the Broker's role in the CDA process. The protocol consists of six messages indicated by the arrows. Listed with each arrow is the information sent. A Client initially supplies the Broker with his/her ID. The Broker signs the Client's ID using its private key. The result is $cert_B(ID)$. The Broker sends a Client Number and $cert_B(ID)$ back to the Client. The rest of the registration procedure is similar to [5].

These modifications allow the Broker to know

every bid the Client submits. This is unavoidable, as the Client must submit his/her bid via the Broker. However, it does ensure that the Broker can't initiate unauthorised trades, as s/he doesn't know the Client's group certificate. This arrangement allows the Broker to perform the bulk of the work in terms of winner determination, research and portfolio management. A Client need only check the Bulletin Board in the case that they wish to verify that his/her bid has been submitted (i.e., neither the Broker nor the Auctioneer is blocking bids). Furthermore, $cert_B(ID)$ allows the Broker to be associated with a bid during tracing.

7 CONCLUSIONS

Online share trading is similar to online auctions. As a result, online share trading exhibits similar privacy and security problems. However, there are more parties involved in the share trading process. This makes defining privacy and security requirements more difficult. Once the pretence of corporate provided security is dropped, the bottom line is parties cannot trust each other. A Client might repudiate having made a bid, or forge bids. Likewise, Brokers may steal payments and execute bogus orders. Existing payment enforcement schemes are restrictive and only provide ad-hoc security. Furthermore, the Auctioneer (i.e., Share Market) can match bids in a non-verifiable manner. The parties involved in the share trading process do not have strong privacy policies. An individual's information can be sold to marketing agencies, or benevolently used against them.

Share market crimes further complicate security matters for CDAs. Insider trading involves using inside knowledge of market sensitive information as the motivation for trading in a particular manner. Misinformation involves deliberately misleading others such that they make an unsound investment, or invest in such a manner that fraudulently benefits the misleader. Existing security mechanisms employed by online Brokers are insufficient and privacy is limited. Regulatory Authorities govern participants and can punish those who engage in criminal or devious behaviour. However, such authorities are expensive to seek recourse through and therefore are largely restricted to policing large-scale fraud. Furthermore, the existence of such an entity also requires the implicit trust of all share market participants.

Cryptographic CDA schemes can prevent many of discussed problems. We show how an existing CDA scheme can be used for secure and private online share trading. Bids are anonymous and the auction process is publicly verifiable. Trust is split between two independent companies, rather than a single trusted Regulatory Authority.

In 1984, David Chaum [1] invented a Digital Cash protocol that allows an individual to spend anonymous cash in a secure manner. Security in auction schemes was not significantly addressed until Franklin and Reiter in 1996 [2]). Cryptographic share market protocols are a logical extension to digital cash. Combining cash-less protocols with auction schemes to construct a secure and anonymous share market, is perhaps the last step in a truly cash-less society.

REFERENCES

[1] D. Chaum, "Security without identification: transaction systems to make Big Brother obsolete," *Communications of the ACM, vol. 29, issue 10, 1985.*

[2] M. Franklin and M. Reiter, "The Design and Implementation of a Secure Auction Service," *IEEE Trans. Software Engineering*, vol. 22, pp. 302-312, 1996.

[3] J. Trevathan, "Security, Anonymity and Trust in Electronic Auctions," *ACM Crossroads*, vol. 11.3, pp. 3-9, 2005.

[4] J. Trevathan, H. Ghodosi, and W. Read, "Design Issues for Electronic Auctions," *Proc. Second Ann. Conf. E-Business and Telecommunications Networks*, pp. 340-347, 2005.

[5] J. Trevathan, H. Ghodosi, and W. Read, "An Anonymous and Secure Continuous Double Auction Scheme," *Proc. Thirty-ninth International Hawaii Conference on System Sciences*, pp. 125 (1-12), 2006.

[6] J. Trevathan and W. Read, "Secure Online Auctions," *Proc. International Conference on Security and Cryptography*, pp. 387-396, 2006.

[7] K. Viswanathan, C. Boyd, and E. Dawson, "A Three Phased Schema for Sealed Bid Auction System Design," *Proc. Australasian Conference on Information Security and Privacy,* vol. 1841 of Lecture Notes in Computer Science, Springer-Verlag, pp. 412-426, 2000.

[8] C. Wang and H. Leung, "Anonymity and Security in Continuous Double Auctions for Internet Retails Market," *Proc. Thirty-seventh International Hawaii Conference on System Sciences*, 2004.

J. Trevathan received his PhD from James Cook University in 2007. He is a lecturer/researcher at James Cook University, an analyst/programmer for Osmotion Pty Ltd, and an Associate Editor for ACM Crossroads. His research interests include privacy, security and fraud prevention methods in e-Commerce applications.

W. Read is an Associate Professor and the Head of the School of Mathematics, Physics and Information Technology at James Cook University. His research interests include mathematical modeling, series solutions and e-Commerce.