al., 1999) and 2-Server (Cachin, 1999) meet this requirement. The \((t,n)\) schemes providing the guarantees as long as a certain proportion of the hosts are not compromised and \((n,n)\) schemes providing the guarantees as long as all of the hosts are compromised.

Even though a distributed scheme is less likely to be compromised, no scheme is perfect so it is still necessary to be able to verify that the auction has been conducted correctly. We may not want to verify each auction; we may only want to audit a proportion to give us confidence. However, we do not want to do this at the expense of bid privacy because we do not want to give advantage to any parties by revealing bid valuations. Schemes that provide these guarantees are: Franklin & Reiter (Franklin & Reiter, 1995), Bidder Resolved (Brandt, 2006), Five Models (Peng et al., 2003), Polynomial (Kikuchi, 2002), Extended HKT (Peng et al., 2002), Verifiable scheme (Parkes et al., 2006), GW Micali (Peng et al., 2005), Yet Another (Ham et al., 2003) and vSGVA (Palmer et al., 2007a).

Grid users will not use any of these schemes if they believe that their privacy is compromised because bid valuations released to the wrong parties can allow them to subvert future auctions. Therefore, strong privacy guarantees are required such as only revealing the winning bidder and the price they paid at the end of the auction while keeping all other bid information secret. Of the schemes meeting our first two criteria, this rules out Franklin & Reiter, Five Models and Verifiable Scheme.

Although the six remaining schemes meet our requirements, the majority only allow auctions for single types of goods. In reality, many Grid resource allocation decisions require determination of allocations of combinations of goods (CAP). At present, the only scheme meeting our requirements and supporting combinatorial auctions is vSGVA. This is an extension of the SGVA (Yokoo & Suzuki, 2002) scheme through the addition of verification.

**FUTURE TRENDS**

As the Grid matures, a vision of a truly global Grid computing infrastructure (Assunção, Buyya, & Venugopal, in press) has started to emerge as a basis for on demand or utility computing. In this global grid computational resources are acquired on demand and provided with an agreed quality of service. This view of the Grid can be further extended from the current institutional model, to one where participation is open to all, and resources may be used or potentially provided by the general public, institutions or companies. The technologies discussed in this chapter, by minimising the need for prearranged trust through a combination of distribution of trust and verification, will enable the emergence of new marketplaces for trading application services, computation, bandwidth and storage within such a global Grid. Looking even further ahead, it is possible to imagine such market oriented technologies underpinning peer based user-centric Grid communities, in which users can contribute and consume computing power on demand, purchase services and collectively provide the computing infrastructure. This could provide resources to support ubiquitous computing scenarios such as those envisioned by the MIT Project Oxygen (Rudolph, 2001).
However much work remains to be done. Additional research needs to be done in providing frameworks and infrastructures to support the development of market oriented Grid Software. More specifically, research needs to be carried out to improve the performance of the auction schemes outlined in this chapter. A number of the verification techniques in this chapter could also be applied to general computation, for example (Min et al., 2005), these could be applied to webservices to verify that they have executed correctly for their given input.

CONCLUSION

On demand (or utility computing) is one of the motivators of the Grid economy, although the same basic economic techniques can be usefully applied for resource allocation in other Grids such as, clusters, scientific Grids and sensor Grids. Underpinning the Grid economy are resource markets and the means of interacting with them. Ultimately a Grid economy represents a paradigm shift within the Grid community, where resources are traded, negotiated, allocated, provisioned, and monitored based on users quality of service requirements. The Grid economy will underpin the evolution of the Grid from a collection of computational islands into a global computational environment capable of delivering different levels of service, risk and cost, depending on the preferences of the user. When the resources being allocated are spread across varied administrative domains and ownership, the allocations of the resource allocator (in our case auctioneer) must provide confidence in the outcome. Essentially economic interactions must provide privacy and trustworthiness before the Grid economy will be widely adopted, especially in a competitive economic environment. Verifiable privacy preserving auctions satisfy these requirements, permitting any Grid or Utility computing provider to hold a resource auction for its (and others’) resources without needing to be trusted or even trustworthy.

REFERENCES


**Terms and Definitions**

**Grid Economy** – The grid economy is a market in which computing resources and services are bought and sold on demand.

**Grid Resource Broker** – A grid resource broker is a grid application scheduler that is responsible for resource discovery, selection, scheduling, and deployment of computations over resources.

**Trust** – Reliance placed on a party for some purpose such as correctly computing an auction result, or not revealing private information.

**Trustworthy** – Deserving of trust, often due to past actions or reputation.

**Encryption** – To alter data using a secret code so that it is unidentifiable to unauthorized parties. Authorized parties can use a code to decrypt the data to its original form.

**Auction** – The sale of some item or items where an auctioneer is selling to a set of bidders who place bids. An auction employs dynamic pricing dependant on the values of the bids.

**Combinatorial Allocation Problem** – How to efficiently allocate the items in a combinatorial auction to the bidders in an optimal way.

**Combinatorial Auction** – An auction where there is more than one heterogeneous item for sale. Bidders can place bids on combinations of specific items.
**Privacy Preserving** – Maintaining the confidential nature of some item. An auction can be said to be privacy preserving if any confidential data sent to the auctioneer that does not need to be revealed to complete the auction remains confidential..

**Verification** – To check that some process has been correctly completed. Verification of an auction involves at the minimum checking that the auction protocol has been correctly executed, and that all bids have been counted..