Towards a Blockchain Ontology

Joost de Kruijff, Hans Weigand,

Tilburg University, P.O. Box 90153
5000 LE Tilburg, The Netherlands
email@joost.xyz, weigand@uvt.nl

Abstract.
Blockchain technology is regarded as highly disruptive, but there is a lack of formalization and standardization of terminology. Not only because there are several (sometimes propriety) implementation platforms, but also because the academic literature so far is predominantly written from either a purely technical or an economic application perspective. The result of the confusion is an offspring of blockchain solutions, types, roadmaps and interpretations. For blockchain to be accepted as a technology standard in established industries, it is pivotal that ordinary internet users and business executives have a basic yet fundamental understanding of the workings and impact of blockchain. This conceptual paper provides a theoretical contribution and guidance on what blockchain actually is by taking an ontological approach. Enterprise Ontology is used to make a clear distinction between the datalogical, infological and essential level of blockchain transactions and smart contracts.

Keywords: Enterprise Ontology, Business Model Ontology, REA, Blockchain

1 Introduction

Blockchain is the emergent technology that people talk about, even though few actually know what the new technology entails in detail [1]. According to [2], blockchain research lacks scientific rigor due to its young age and is primarily concerned with what blockchain could become as a disruptive technology for the Internet of Things (IoT). As common with emerging technologies, multiple interpretations and the absence of a formal model and terminology exist that can be applied for research purposes. Against this background, this short paper aims to provide a theoretical contribution and guidance on what blockchain actually is instead of what it could become by using an ontological approach.

Ontology has been recognized as a useful instrument for reducing conceptual ambiguities and inconsistencies while identifying value-creating capabilities in a certain domain [11]. Ontology is becoming an increasingly important instrument for reducing complexity by structuring domains of interests [12]. According to the popular OntoClean methodology [13], domain structuring starts with the identification of a set of classes in a taxonomy, followed by assigning metaproperties for each property. Then, it needs to be verified whether constraints are violated by these metaproperties.

Ontology design only makes sense once the designer and audience have basic yet fundamental understanding about the subject of analysis, blockchain. In essence, blockchain is a distributed consensus system for parties, that do not trust each other, to transact. Hereby, blockchain differentiates from traditional transaction systems with respect to how it irreversibly stores transaction data in a distributed ledger. Once verified (mined or validated) and stored, there is no way to manipulate data on the blockchain, as changes are immediately reflected in all active copies of the ledger across the network. Blockchain comes in three forms; *public*, *private* or *hybrid* [3]. Their functioning is explained in Fig. 1.

Consensus	Type	Governance	Trust	Scalability	Use
Decentralized, based on proof	Public, Not permissioned	Anonymous nodes	Low	Limited	e.g. Virtual currency
Hybrid, based on validation	Consortium, Private, Permissioned	Pre-selected set of nodes	Medium	Unlimited	e.g. Banking system
Centralized, based on validation	Private, Permissioned	Single organization	High	Unlimited	e.g. Government, notary

Fig.1. Common terminology for blockchain constructs

Besides the information systems' perspective, our blockchain ontology should also relate to the business operation and processes of potential enterprise adopters. Enterprise ontology provides a collection of relevant terms and natural language definitions. Well-known examples of enterprise ontology frameworks are TOVE, EO [14] and the Enterprise Ontology of DEMO [15]. DEMO is inspired by the language/action perspective, which has been initially developed as a philosophy of language derived from the speech act theory [16]. It is based on explicit specified axioms characterized by a rigid modeling methodology [17], and is focused on the construction and operation of a system rather than the functional behavior. It emphasizes the importance of choosing the most effective level of abstraction during information system development in order to establish a clear separation of concerns [18]. As DEMO has been proven to be a helpful methodology to formalize systems that are ambiguous, inconsistent or incomplete [17], especially when it comes to reducing modeling complexity [19], this short paper will use Enterprise Ontology and DEMO to describe the blockchain ontology from a datalogical, infological and essential (business) perspective.

The structure of this paper is as follows. Section 2 presents a blockchain ontology using the three levels of abstraction of Enterprise Ontology. In section 3, we use this ontological analysis to compare blockchain to existing Information Systems. The research outcomes and directions for future research conclude this paper in Sections 4.

2 Designing a blockchain ontology

An important development in the history of databases in the early '70s was the separation of implementation choices from the database conceptual model (the principle of data independence). We believe that a similar separation is highly needed for the blockchain domain. We propose to adopt the distinction axiom of Enterprise Ontology as ontological basis for this separation.

The distinction axiom of Enterprise Ontology distinguishes three basic human abilities: performa, informa, and forma [15]. The *forma* ability concerns the form aspects of communication and information. Production acts at the forma level are datalogical in nature: they store, transmit, copy, destroy, etc. data. The *informa* ability concerns the content aspects of communication and information. Production acts at the forma level are infological in nature, meaning that they reproduce, deduce, reason, compute, etc. information, abstracting from the form aspect. The *performa* ability concerns the bringing about of new, original things, directly or indirectly by communication. Communicative acts at the performa level are about evoking or evaluating commitment; these communicative acts are realized at the informa level by means of messages with some propositional content.

The distinction axiom is highly relevant for blockchain. Following the three abilities, we distinguish three ontological layers (Fig.2). We start from the datalogical layer that describes blockchain transactions at the technical level in terms of blocks and code. From there, we make an infological abstraction in order to describe the blockchain transactions as effectuating an (immutable) open ledger system. This layer aims to abstract from the various implementations that exist today or will be developed in the future. To describe the economic meaning of the

infological transactions we use the essential layer. This is the preferred level of specification for a blockchain application as it abstracts from the implementation choices.

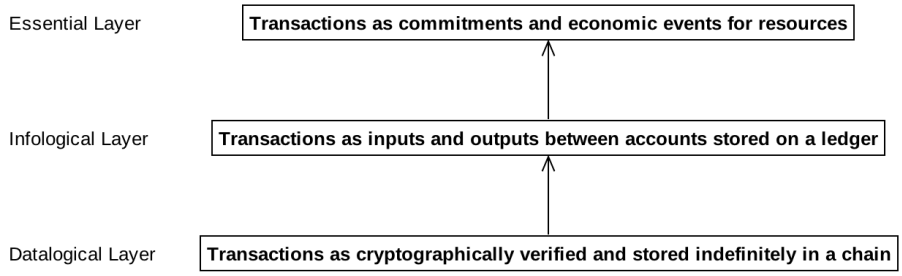

Fig. 2. Enterprise Ontology layers applied to blockchain transactions

2.1 Datalogical blockchain ontology

In most of the publications on blockchain the concept is described in terms of the technology that is used, that is, in terms of blocks, miners, mainchains, sidechains etc. This technological basis is to be positioned at the datalogical level, the level of data structures and data manipulation. To build a blockchain domain ontology for this level we have used taxonomies as identified in cryptocurrency [4], blockchain research [21] and technical implementations by blockchain- and cloud providers [5].

Several specialized ontology languages are available nowadays, but one of most wide-spread modeling approaches is Object Management Group's Unified Modeling Language (UML), together with Object Constraint Language (OCL) [22], making it the best fit for our blockchain ontology. Central to this domain ontology (Fig. 3) are the wallet, transaction and the node. Each blockchain concept relies on these concepts, whereby a transaction can be either simple or contain executable smart contract code. Interactions with the blockchain (from outside the ecosystem) occur through nodes (via runtimes and middleware) by means of API's and sockets, or via sidechains directly, which is our next focus.

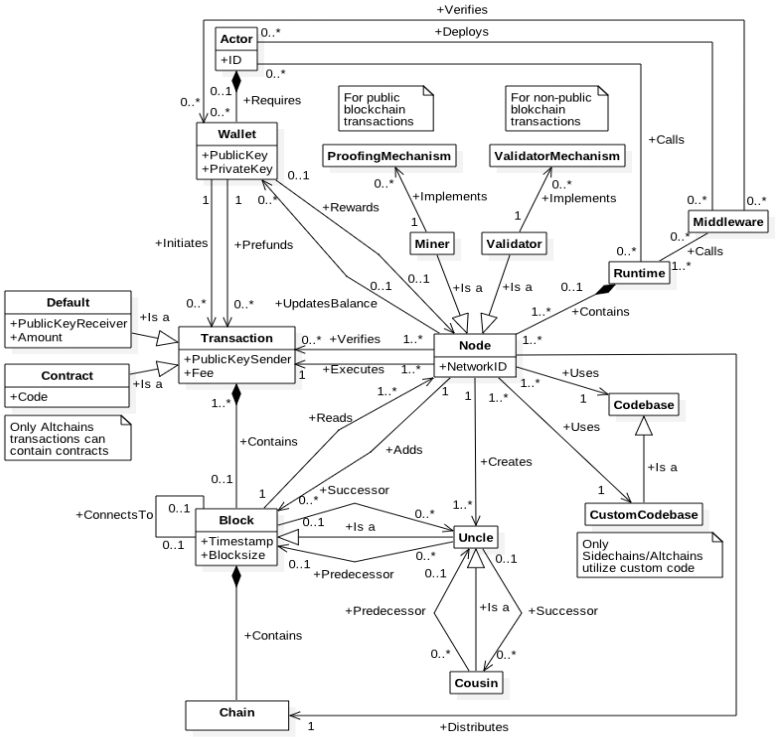

Fig. 3. Datalogical Domain Ontology for a Blockchain Transaction

Figure 4 shows the datalogical taxonomy for chains and chain interactions. A chain can be either a mainchain or a sidechain. Sidechains are always related to one or more mainchains for enhanced functionality. In this overview, a Blockchain should not be confused with the blockchain as a concept, but must be read as the Blockchain as implemented by Bitcoin. Although not included in the ontology, technical off-chain solutions living outside the blockchain ecosystem may become an entity of significance in the future, as governments and enterprises build infrastructures consisting non-vital information (like master data) and capable of interacting with blockchain.

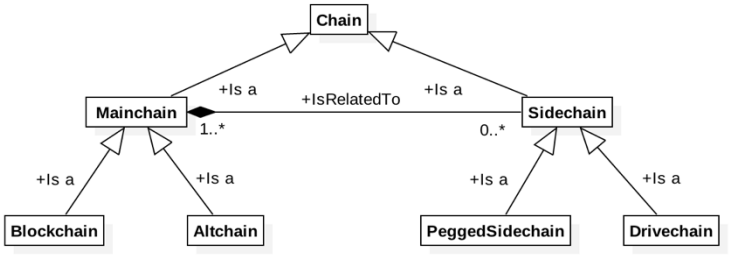

Fig. 4. Datalogical Domain Taxonomy for the Blockchain Ecosystem

2.2 Infological Blockchain Ontology

In the 1970s, Langefors was the first to make the important distinction between information (as knowledge) and data (as representation) [25]. This separation of content and form created a new field in knowledge engineering called Infology, aimed to make complicated structures intellectually manageable [15].

When blockchain is described in the current literature as a "distributed ledger" [26], this is an infological characterization that abstracts from the encrypted data blocks, miners, chains, etcetera that make up the datalogical level. A transaction, in this ledger system, is not just a block of data, but a transfer of some value object (e.g. Bitcoin). A ledger consists of *accounts* (e.g. debit

account), and this concept is indeed generic across the majority of blockchain providers that are part of this analysis. Accounts are not limited to have a (crypto) currency- balance or quantity, but may also refer to other types like stocks or a claim as mainchains other than Bitcoin (not taking sidechains into account) allow to register custom account types.

We made a distinction between journals and ledgers. In a traditional accounting system, journals and ledgers reside where business transactions are recorded. In essence, detail-level information for individual transactions is stored in one of several possible journals, while the information in the journals is then summarized and transferred (or posted) to a ledger. In the blockchain context, such a division can be maintained (and supported at the datalogical level by a combination of mainchain and sidechain), but it is also possible to see the ledger as an aggregated view on the journal. Anyway, the term "ledger" typically refers to a subset of all accounts. For that reason, we have modeled the ledger here as a set of accounts where we do not require every account to be part of a ledger.

Transactions must comply with rules of engagement. One axiomatic rule of engagement in blockchain is that for each transaction, input equals output (debit = credit).

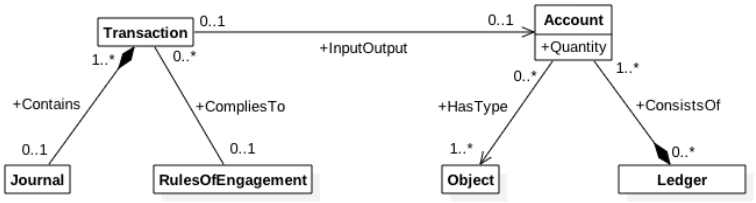

Fig. 5. Infological Ontology for a Blockchain transaction

2.3 Essential Blockchain Ontology

The essential or business level is concerned with what is created directly or indirectly by communication. In the Language/Action Perspective [16], the key notion in communication is commitment as a social relationship based on shared understanding of what is right and what is true. Communicative acts typically establish or evaluate commitments. In a narrower sense, a commitment (promise, commissive) is about what an actor is bound to do (so what is right in a future situation). Such a commitment being agreed upon by two parties is a change in the social reality, as is the agreed upon fulfillment of that commitment.

Given the institutional context to be in place, an infological blockchain transaction moving some value from one account to another represents a change in this social reality (e.g. transfer of ownership). Such a change is what we identify as the essential blockchain transaction.

Enterprise Ontology is not specific about the content of the change. For that reason, we combine Enterprise Ontology with the Business Ontology of REA [28]. The REA model developed by Bill McCarthy [29] can be viewed as a domain ontology for accounting. REA intends to be the basis for integrated accounting information systems focused on representing increases and decreases of value within an organization or beyond. REA inherits the stock-flow nature of accounting, but lifts the syntactic structure of accounts to a semantic level of resources and events.

The accounting perspective is quite appropriate in the blockchain context. Blockchain is facilitating and recording (in an immutable and transparent way) value transfers between economic actors in a shared data environment while accountants (and their customers) are interested in reliable information on these transfers and the resulting value positions of actors. As a blockchain transaction is concerned with events that trigger changes in economic reality (e.g. the value position of actors), REA is perceived to be a better fit for analysis at the essential level than DEMO, which is more concerned with the coordination of these events, which is less significance for blockchain.

REA atomic constituents of processes are called economic *events*. Economic events are carried out by *agents* and affect a certain *resource*, like a (crypto) currency or physical good. The relationship between an economic event and a resource is called *stock-flow*. REA presents five

generalized stock-flows: produce, use, consume, give and take. These stock-flows can generate value flows by conversion (produce, use and consume) or exchange (give and take). In the REA independent view, the give, use and consume stock-flows are process inputs (provide) and produce and take are process outputs (receive). The duality axiom says that provides and receives are always in balance. For instance, in a physical conversion process, some resources are used or consumed in the process of producing other resources. In our blockchain ontology, we will use the term "transaction" to represent such a combination of provide and receive events.

REA includes also the notion of *contract* as a bundle of reciprocal commitments. Following REA and Enterprise Ontology, we have both transactions and commitments. Transactions can exist on their own, for instance, an instant bitcoin transfer from one party to another, but also be part of a contract. A special feature of a *smart* contract (originally introduced by Nick Szabo [27]) is that at least some of the commitments are executed automatically. In this case, the commitments are *self-fulfilling*; the committed transactions are irreversibly saved on the blockchain and executed once certain conditions are matched. This is a very powerful concept as the contract no longer has to rely on trust or complicated trade procedures.

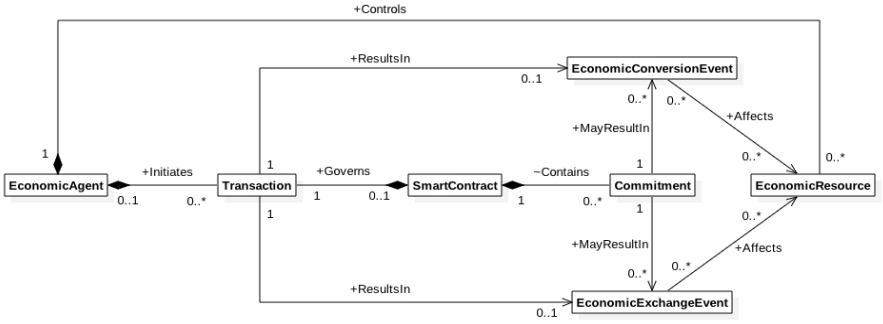

Fig. 6. Essential Ontology of a blockchain transaction

Business transactions are realized in the blockchain by a set of infological transactions, typically one for each outflow/inflow pair. Commitments are also realized by infological transactions – in this case, a transfer to a commitment type account. The fulfillment is realized by a transfer from that commitment type account. The difference between conversions and exchanges is that in the latter case, the provided resource is the same as the received resource, while they are different in the former case.

A common ambiguity of blockchain processing is within its scope, concerned with the extent of a conversion- or exchange process that is processed on the blockchain (internal) or beyond (external), also referred to as on-/offchain processing. With reference to REA processes, it can be stated that the planning (creation of a smart contract) and the allocation of input resources (outflow events) materialize on the blockchain, whereas the contract execution by means of exchange- and conversion (to a lesser extent), triggers output resources (inflow events) that may have reach outside the blockchain, even to physical entities, like for example IoT devices. This capability is regarded as a major advantage to risky physical services (e.g. car rental) and services that can now combine blockchains immutable data capability while utilizing their own (industry specific) processes to safely deliver a service (e.g. charging of harbour fares to freighters based on a GPS record on blockchain).

3 Discussion

This paper applied the concept of abstraction on the blockchain concept utilizing Enterprise Ontology. The chosen structure aimed to explain blockchain with maximum separation of concern with regards to substance, context and audience. It turns out that a blockchain transaction, regardless of its complex ecosystem and cryptographical ingredients at the datalogical layer, shows significant infological and essential conceptual similarities with traditional economic transactions as used today.

However, although the concepts are not different, their properties change. It makes a difference when mutable records are replaced by immutable records, and when the fulfilment of commitments is left to the infrastructure rather than to the voluntary acts of the parties. Fig. 11 summarizes a comparison between blockchain and traditional transaction systems.

	Blockchain	**Traditional**
Essential	Communication success based on non-tamperable infrastructure	Communication success based on subjective and objective trust (control procedures)
Infological	Performative transactions integrating descriptive and prescriptive	Descriptive transactions (to be verified) and prescriptive transactions (to be realized and evaluated)
Datalogical	Immutable records (based on consensus mechanism), stored outside the company	Mutable records (to be protected), stored within the companies

Fig. 7. Comparison between blockchain and traditional transaction systems

At the datalogical level, the difference is not only that records become immutable, but also that the transaction databases get positioned in between companies, rather than inside companies, thus removing data redundancy that exists today (although another form of redundancy is introduced in the consensus mechanisms). On the infological level, control procedures are not relevant anymore. An interesting feature of blockchain transactions is that they are not just a description of some transfer (e.g. of Bitcoins) but the very existence of the transfer depends on this description. This performative property also applies to other transactions, like service deliveries, when the blockchain is tightly coupled with IoT services, and to commitments (their bare existence). At the essential level, smart contracts also add the automatic fulfillment of commitments, and more in general, there is a change in what makes the communication successful: trust, perhaps grounded in control procedures, or the impersonal and non-tamperable infrastructure.

4 Conclusion

This short paper describes an initial blockchain ontology on three levels. As such, it supports a better understanding of this disruptive technology. It also can be used to support application development, as it suggests to specify the blockchain application on the business level first. In our view, it should be possible then to generate the blockchain implementation automatically, with some design parameters to be set. For the specification of the business level, in terms of contract languages and graphical formats, it is possible to draw on already proven modeling approaches.

We have not provided an extensive validation of the ontology yet, so the proposed model should be regarded as initial. Apart from the formal verification using top ontologies like DOLCE, further validation is to be done with applications as well as by establishing mappings to the various blockchain implementations that exist. We cannot claim that the present model is complete and conclusive, but at least it provides a first reference point.

The current ontology does not stop the need for further research on blockchain technology of course. On the contrary, an important next step is to understand and formalize interactions between mainchains, sidechains and off-chains within or across the public, private and hybrid domain (blockchain zoning), to mention one issue. Separating the goal – immutable transactions, smart contracts – from the implementation can help to better explore all implementation variants without dogmatism.

References

1. Swanson T.: Consensus-as-a-service: a brief report on the emergence of permissioned, distributed ledger systems, 2015

2. Pilkington M.: Blockchain Technology: Principles and Applications, Research Handbook on Digital Transformations, September 2015 9. Robert Baldwin & Martin Cave (1999), Understanding Regulation: theory, strategy and practice. Oxford UP.
3. Buterin V.: On Public and Private Blockchains, crypto renaissance salon, August 7, 2015
4. Glaser F., Bezzenberger L.: Beyond Cryptocurrencies – A Taxonomy of Decentralized Consensus Systems, 23rd European Conference on Information Systems (ECIS 2015), 2015
5. Gray M.: Introducing Project Bletchley (Microsoft), June 2016
6. Tschorsch F., Scheuermann B.: Bitcoin and Beyond. Cryptology ePrint Archive IACR, Berlin 2015, page 464
7. Chaum, D: Blind Signatures for Untraceable Payments. Advances in Cryptology, 1983, pages 199-20
8. Scott, B: Visions of a Techno-Leviathan: The Politics of the Bitcoin Blockchain. E-International Relations, June 2014 6.
9. Böhme R., Christin N., Edelman B., Moore, T.: Bitcoin: Economics, Technology, and Governance. Journal of Economic Perspectives, Vol. 29, Issue 2 - Spring 2015
10. Wright A. and De Filippi P.: Decentralized Blockchain Technology and the Rise of Lex Cryptographia, March 2015.
11. Guarino N., Oberle, D and Staab, S: What Is an Ontology, 2009
12. Noy, N., McGuinness D., Ontology Development 101: A Guide to Creating Your First Ontology, Semantic Web Working Symposium, 2001
13. Guarino, N.; Formal ontology and information system, Proceedings of FOIS, 1998
14. Andersson, B., Bergholtz M., Edirisuriya A., Ilayperuma T., Johannesson P., Gordijn J., Grégoire B., Schmitt M., Dubois, E., Abels S., Hahn A., Wangler, B., Weigand H.: Towards a Reference Ontology for Business Models, Volume 4215 of the series Lecture Notes in Computer Science pp 482-496
15. Dietz J.: Enterprise Ontology, Springer 2006
16. Weigand, H. & de Moor, A.: Argumentation semantics of communicative action, Proceedings of the 9th International Working Conference on the Language-Action Perspective of Communication Modelling (LAP 2004). Aakhus, M. & Lind, M. (eds.). New Brunswick, NJ: International Working Conference on the LAP on Communication, p. 159-178, 2004
17. Nuffel D., Mulder H., van Kervel S.: Enhancing the Formal Foundations of BPMN by Enterprise Ontology, Advances in Enterprise Engineering III, 5th International Workshop, CIAO! 2009, and 5th International Workshop, EOMAS 2009, held at CAiSE 2009, Amsterdam, The Netherlands, June 8-9, 2009
18. den Haan, J.: Modeling an Organization using Enterprise Ontology, 2009
19. Wang Y., Albani A., Barjis J.: Transformation of DEMO Metamodel into XML Schema, Advances in Enterprise Engineering V Volume 79 of the series Lecture Notes in Business Information Processing pp 46-60, 2011
20. Mainelli, M., Smith M.: Sharing ledgers for sharing economies: an exploration of mutual distributed ledgers (aka blockchain technology), The Journal of Financial Perspectives: FinTech, Winter 2015 | Volume 3 – Issue 3
21. Christidis K., Devetsikiotis M.: Blockchains and Smart Contracts for the Internet of Things, Special Section on the Plethora of Research in Internet of Things (IoT), April 23, 2016
22. Cranefield S., Purvis M.; UML as an Ontology Modelling Language, The Information Science: Discussion Paper Series, Number 99/01, January 1999
23. Lerner S.: Drivechains, Sidechains and Hybrid 2-way peg Designs, 2016
24. Back A., Corallo M., Dashjr L., Friedenbach M., Maxwell G., Miller A., Poelstra A., Timón J., and Wuille P.: Enabling Blockchain Innovations with Pegged Sidechains, 2014
25. Goldkuhl G.: Information as Action and Communication, The Infological Equation, Essays in honour of B. Langefors, B. Dahlbom (ed.), Gothenburg Studies in Information Systems, Gothenburg Univ, 1995. (also: Linkoping Univ report LiTH-IDA-R-95-09)
26. UK Government Office for Science: Distributed Ledger Technology: Beyond the Blockchain, 2015
27. Szabo, N.: Formalizing and securing relationships on public networks. First Monday 2, no. 9, 1997
28. Hunka, F., Zácek, J.: A new view of REA state machine. Applied Ontology 10(1): 25-39, 2015
29. McCarthy W.: The REA Accounting Model: A Generalized Framework for Accounting Systems in a Shared Data Environment, The Accounting Review, Vol. LVII, No. 3, July 1982