A bill to be entitled
An act relating to information technology; amending s. 282.0051, F.S.; revising certain powers, duties, and functions of the Agency for State Technology in collaboration with the Department of Management Services; amending s. 282.201, F.S.; authorizing the state data center within the agency to extend, up to a specified timeframe, certain service-level agreements; requiring the state data center to submit a specified report to the Executive Office of the Governor under certain circumstances; deleting a requirement for a service-level agreement to provide a certain termination notice to the agency; requiring the state data center to plan, design, and conduct certain testing, if cost-effective; deleting obsolete provisions relating to the schedule for consolidations of agency data centers; conforming provisions to changes made by the act; amending s. 322.032, F.S.; directing the Department of Highway Safety and Motor Vehicles, in collaboration with the Agency for State Technology, to implement protocols and standards for issuing an optional digital proof of driver license, enter into a contract for a specified purpose, and procure certain interfaces necessary for authorized private entities to consume a digital proof of driver license.
license; requiring the agency, in collaboration with the department, to maintain and publish such protocols and standards; requiring the agency to timely review and approve all private entity requests for authorized access to certain interfaces that meet the agency's requirements; providing that agency approval of such access designates the approved entity as an authorized consumer of digital proofs of driver licenses; providing for revenue sharing between such authorized manufacturer and the state; requiring deposit of the state share of such revenue in the Highway Safety Operating Trust Fund; requiring the agency, in collaboration with the department, to enter into a specified agreement with such authorized manufacturer; requiring that a digital proof of driver license be in a format that allows law enforcement to verify the authenticity of such digital proof of driver license; providing that presenting an electronic device displaying a digital proof of driver license does not constitute consent for a law enforcement officer to access any other information on such device; providing for the assumption of liability; amending s. 668.50, F.S.; providing and revising definitions; providing that a contract may not be denied legal effect or enforceability solely because it includes a smart
contract term; providing that rights of ownership or
use of certain information are not affected by the use
of blockchain technology to secure such information;
providing an effective date.

Be It Enacted by the Legislature of the State of Florida:

Section 1. Subsection (18) of section 282.0051, Florida
Statutes, is amended to read:

282.0051 Agency for State Technology; powers, duties, and
functions.—The Agency for State Technology shall have the
following powers, duties, and functions:

(18) In collaboration with the Department of Management
Services:

(a) Establish an information technology policy for all
information technology-related state contracts, including state
term contracts for information technology commodities,
consultant services, and staff augmentation services. The
information technology policy must include:

1. Identification of the information technology product
and service categories to be included in state term contracts.

2. Requirements to be included in solicitations for state
term contracts.

3. Evaluation criteria for the award of information
technology-related state term contracts.
4. The term of each information technology-related state term contract.
5. The maximum number of vendors authorized on each state term contract.
   (b) Evaluate vendor responses for information technology-related state term contract solicitations and invitations to negotiate.
   (c) Answer vendor questions on information technology-related state term contract solicitations.
   (d) Ensure that all information technology-related solicitations by the department are procured and state contracts are managed in accordance with the information technology policy established under pursuant to paragraph (a) is included in all solicitations and contracts which are administratively executed by the department.

Section 2. Paragraph (d) of subsection (2) of section 282.201, Florida Statutes, is amended, paragraph (g) is added to that subsection, and subsection (4) of that section is amended, to read:

282.201 State data center.—The state data center is established within the Agency for State Technology and shall provide data center services that are hosted on premises or externally through a third-party provider as an enterprise information technology service. The provision of services must comply with applicable state and federal laws, regulations, and
policies, including all applicable security, privacy, and auditing requirements.

(2) STATE DATA CENTER DUTIES.—The state data center shall:

(d) Enter into a service-level agreement with each customer entity to provide the required type and level of service or services. If a customer entity fails to execute an agreement within 60 days after commencement of a service, the state data center may cease service. A service-level agreement may not have an original term exceeding 3 years, but the service-level agreement may be extended for up to 6 months. If the state data center and an existing customer entity either execute an extension or fail to execute a new service-level agreement before the expiration of an existing service-level agreement, the state data center must submit a report to the Executive Office of the Governor within 5 days after the date of the executed extension or 15 days before the scheduled expiration date of the service-level agreement, as applicable, to explain the specific issues preventing execution of a new service-level agreement and to describe the plan and schedule for resolving those issues. A service-level agreement, and at a minimum, must:

1. Identify the parties and their roles, duties, and responsibilities under the agreement.

2. State the duration of the contract term and specify the conditions for renewal.
3. Identify the scope of work.

4. Identify the products or services to be delivered with sufficient specificity to permit an external financial or performance audit.

5. Establish the services to be provided, the business standards that must be met for each service, the cost of each service, and the metrics and processes by which the business standards for each service are to be objectively measured and reported.

6. Provide a timely billing methodology to recover the cost of services provided to the customer entity pursuant to s. 215.422.

7. Provide a procedure for modifying the service-level agreement based on changes in the type, level, and cost of a service.

8. Include a right-to-audit clause to ensure that the parties to the agreement have access to records for audit purposes during the term of the service-level agreement.

9. Provide that a service-level agreement may be terminated by either party for cause only after giving the other party and the Agency for State Technology notice in writing of the cause for termination and an opportunity for the other party to resolve the identified cause within a reasonable period.

10. Provide for mediation of disputes by the Division of Administrative Hearings pursuant to s. 120.573.
(g) Plan, design, and conduct testing with information technology resources to implement services within the scope of the services provided by the state data center, if cost-effective.

(4) SCHEDULE FOR CONSOLIDATIONS OF AGENCY DATA CENTERS.—

(a) Consolidations of agency data centers and computing facilities into the state data center shall be made by the dates specified in this section and in accordance with budget adjustments contained in the General Appropriations Act.

(b) During the 2013-2014 fiscal year, the following state agencies shall be consolidated by the specified date:

1. By October 31, 2013, the Department of Economic Opportunity.

2. By December 31, 2013, the Executive Office of the Governor, to include the Division of Emergency Management except for the Emergency Operation Center's management system in Tallahassee and the Camp Blanding Emergency Operations Center in Starke.

3. By March 31, 2014, the Department of Elderly Affairs.

4. By October 30, 2013, the Fish and Wildlife Conservation Commission, except for the commission's Fish and Wildlife Research Institute in St. Petersburg.

(a)-(e) The following agency data centers are exempt from state data center consolidation under this section: the Department of Law Enforcement, the Department of the Lottery's...
Gaming System, Systems Design and Development in the Office of Policy and Budget, the regional traffic management centers as described in s. 335.14(2) and the Office of Toll Operations of the Department of Transportation, the State Board of Administration, state attorneys, public defenders, criminal conflict and civil regional counsel, capital collateral regional counsel, and the Florida Housing Finance Corporation.

(b)(d) A state agency that is consolidating its agency data center or computing facility into the state data center must execute a new or update an existing service-level agreement within 60 days after the commencement of the service. If a state agency and the state data center are unable to execute a service-level agreement by that date, the agency shall submit a report to the Executive Office of the Governor within 5 working days after that date which explains the specific issues preventing execution and describing the plan and schedule for resolving those issues.

(c)(e) Each state agency consolidating scheduled for consolidation into the state data center shall submit a transition plan to the Agency for State Technology by July 1 of the fiscal year before the fiscal year in which the scheduled consolidation will occur. Transition plans must be developed in consultation with the state data center and must include:

1. An inventory of the agency data center's resources
being consolidated, including all hardware and its associated
life cycle replacement schedule, software, staff, contracted
services, and facility resources performing data center
management and operations, security, backup and recovery,
disaster recovery, system administration, database
administration, system programming, job control, production
control, print, storage, technical support, help desk, and
managed services, but excluding application development, and the
agency's costs supporting these resources.

2. A list of contracts in effect, including, but not
limited to, contracts for hardware, software, and maintenance,
which identifies the expiration date, the contract parties, and
the cost of each contract.

3. A detailed description of the level of services needed
to meet the technical and operational requirements of the
platforms being consolidated.

4. A timetable with significant milestones for the
completion of the consolidation.

(d) Each state agency consolidating scheduled for
consolidation into the state data center shall submit with its
respective legislative budget request the specific recurring and
nonrecurring budget adjustments of resources by appropriation
category into the appropriate data processing category pursuant
to the legislative budget request instructions in s. 216.023.

Section 3. Subsections (1) and (2) of section 322.032,
Florida Statutes, are amended to read:

322.032  Digital proof of driver license.—

(1)(a)  The department, in collaboration with the Agency for State Technology, shall establish and implement protocols and standards for issuing an optional digital proof of driver license, contract with a private entity to serve as the authorized manufacturer of a digital proof of driver license, and procure any application programming interface necessary for enabling qualified and authorized private entities to securely consume a digital proof of driver license. The department may contract with one or more private entities to develop a digital proof of driver license system.

(b)  The Agency for State Technology, in collaboration with the department, shall maintain and publish on its website the protocols and standards necessary for a private entity to request authorized access to an application programming interface necessary for such private entity to consume a digital proof of driver license. The agency shall timely review requests for authorized access and must approve all requests by private entities that meet the agency's requirements. The agency's approval of a request for authorized access designates the private entity that made the request as an authorized consumer of digital proofs of driver licenses.

(c)  Revenue generated from the manufacture or consumption of
of a digital proof of driver license must be collected by the authorized manufacturer of digital proofs of driver licenses and such revenue must be shared with the state on a revenue-sharing basis. Such authorized manufacturer is responsible for remitting 50 percent of all revenue collected for deposit into the Highway Safety Operating Trust Fund. The Agency for State Technology, in collaboration with the department, shall enter into an agreement with the authorized manufacturer that provides the permitted uses, terms and conditions, privacy policy, and uniform remittance terms relating to the consumption of a digital proof of driver license.

(2) (a) The digital proof of driver license developed by the department or by an entity contracted by the department must be in such a format as to allow law enforcement to verify the authenticity of the digital proof of driver license. The department may adopt rules to ensure valid authentication of a digital proof of driver license by law enforcement.

(b) The act of presenting to a law enforcement officer an electronic device displaying a digital proof of driver license does not constitute consent for the officer to access any information on the device other than the digital proof of driver license.

(c) The person who presents the device to the officer assumes liability for any resulting damage to the device.

Section 4. Subsection (20) of section 668.50, Florida
Statutes, is renumbered as subsection (21), subsection (2) and paragraph (b) of subsection (7) are amended, and a new subsection (20) is added to that section, to read:

668.50 Uniform Electronic Transaction Act.—

(2) DEFINITIONS.—As used in this section:

(a) "Agreement" means the bargain of the parties in fact, as found in their language or inferred from other circumstances and from rules, regulations, and procedures given the effect of agreements under provisions of law otherwise applicable to a particular transaction.

(b) "Automated transaction" means a transaction conducted or performed, in whole or in part, by electronic means or electronic records, in which the acts or records of one or both parties are not reviewed by an individual in the ordinary course in forming a contract, performing under an existing contract, or fulfilling an obligation required by the transaction.

(c) "Blockchain technology" means distributed ledger technology that uses a distributed, decentralized, shared, and replicated ledger, which may be public or private, permissioned or permissionless, and driven by tokenized crypto-economics or tokenless. The data on the ledger must be immutable, auditable, protected with cryptography, and provide an uncensored truth.

(d) "Computer program" means a set of statements or instructions to be used directly or indirectly in an information processing system in order to bring about a certain result.
"Contract" means the total legal obligation resulting from the parties' agreement as affected by this act and other applicable provisions of law.

"Electronic" means relating to technology having electrical, digital, magnetic, wireless, optical, electromagnetic, or similar capabilities.

"Electronic agent" means a computer program or an electronic or other automated means used independently to initiate an action or respond to electronic records or performances in whole or in part, without review or action by an individual.

"Electronic record" means a record created, generated, sent, communicated, received, or stored by electronic means. A record or contract that is secured through blockchain technology is in an electronic form and is an electronic record.

"Electronic signature" means an electronic sound, symbol, or process attached to or logically associated with a record and executed or adopted by a person with the intent to sign the record. A signature that is secured through blockchain technology is in an electronic form and is an electronic signature.

"Governmental agency" means an executive, legislative, or judicial agency, department, board, commission, authority, institution, or instrumentality of this state, including a county, municipality, or other political subdivision.
of this state and any other public or private agency, person,
partnership, corporation, or business entity acting on behalf of
any public agency.

(k) "Information" means data, text, images, sounds,
codes, computer programs, software, databases, or other similar
representations of knowledge.

(l) "Information processing system" means an electronic
system for creating, generating, sending, receiving, storing,
displaying, or processing information.

(m) "Person" means an individual, corporation, business
trust, estate, trust, partnership, limited liability company,
association, joint venture, governmental agency, public
corporation, or any other legal or commercial entity.

(n) "Record" means information that is inscribed on a
tangible medium or that is stored in an electronic or other
medium and is retrievable in perceivable form, including public
records as defined in s. 119.011.

(o) "Security procedure" means a procedure employed for
the purpose of verifying that an electronic signature, record,
or performance is that of a specific person or for detecting
changes or errors in the information in an electronic record.
The term includes a procedure that requires the use of
algorithms or other codes, identifying words or numbers,
encryption, or callback or other acknowledgment procedures.

(p) "Smart contract" means an event-driven program that
runs on a distributed, decentralized, shared, and replicated ledger and can take custody over and instruct the transfer of assets on that ledger.

(q) "State" means a state of the United States, the District of Columbia, Puerto Rico, the United States Virgin Islands, or any territory or insular possession subject to the jurisdiction of the United States. The term includes an Indian tribe or band, or Alaskan native village, which is recognized by federal law or formally acknowledged by a state.

(r) "Transaction" means an action or set of actions occurring between two or more persons relating to the conduct of business, commercial, insurance, or governmental affairs.

(7) LEGAL RECOGNITION OF ELECTRONIC RECORDS, ELECTRONIC SIGNATURES, AND ELECTRONIC CONTRACTS.—

(b) A contract may not be denied legal effect or enforceability solely because:

1. An electronic record was used in the formation of the contract.

2. The contract contains a smart contract term.

(20) RIGHTS OF OWNERSHIP OR USE.—Notwithstanding any law, rule, or regulation to the contrary, the use of blockchain technology to secure information while engaged in interstate or foreign commerce does not affect the rights of ownership or use held by the owner of such information unless the terms of the transaction expressly provide for the transfer of such rights.
Section 5. This act shall take effect July 1, 2018.